Ahmed Alshehri*, Joseph Spielman, Amiya Prasad, and Chuan Yue*

# Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of Both Owners and Bystanders

**Abstract:** Smart home IoT devices collect data not only from owners of the devices, but also from bystanders in a smart home (e.g., visiting family members, friends, or domestic workers). Existing research mainly considered the privacy concerns of bystanders from their own perspectives. In this paper, we design and conduct a survey study to more comprehensively explore the privacy concerns of bystanders from the perspectives of both owners and bystanders. For owners, we investigate their understanding of their own data practices, their views on bystanders' privacy, and their willingness to negotiate data practices with bystanders. For bystanders, we investigate their privacy concerns, their expectations of disclosures by owners, and their willingness to share their data with owners. We recruited 200 owners and 100 bystanders. We found that most owners of smart homes recognize the privacy rights of bystanders, do not fully understand their own data practices, and are willing to address the privacy concerns of trusted bystanders. We also found that most bystanders have concerns about their privacy in other people's smart homes, do not expect owners to disclose data practices, and are willing to share data about them with owners if they consent. Reaching a temporary agreement about data practices between owners and bystanders might require some negotiation. So, we also explore the willingness of owners and bystanders on negotiating data collection, storage, and sharing in smart homes. We found that many owners and bystanders have different preferences regarding negotiating data practices. Based on our findings, we provide recommendations for enhancing the privacy protection in smart homes.

**Keywords:** Privacy, Smart home devices, Owners, Bystanders

DOI 10.56553/popets-2022-0064
Received 2021-11-30; revised 2022-03-15; accepted 2022-03-16.

## 1 Introduction

Smart home devices have been widely adopted in recent years, with 69% of households in the United States having at least one smart home device [35]. Three out of five Americans own smart home devices intended for security purposes, but smart home devices' security and other services are currently designed with mainly the owners in mind [9]. This can lead to problems because owners can have bystanders (e.g., visiting family members, friends, or domestic workers such as plumbers) in their smart homes, whose privacy rights could be infringed upon due to the various forms of data that could be collected about them without their consent [7, 43].

Recently researchers began to study bystanders' privacy from two angles. Some researchers only focused on understanding bystanders' privacy concerns (e.g., [7, 11, 20, 43]). However, owners' perspectives of bystanders' privacy concerns were missing in these studies. Owners are the decision makers in smart homes, not bystanders. For example, if a bystander is uncomfortable about some data collection and wishes to stop the collection, we do not know if the owner would address the bystander's concerns or not. Some other researchers focused on proposing tools for bystanders to protect their privacy in public areas (e.g., campuses in [17, 29]). However, expectations of privacy differ between public and private (e.g., homes) places [18, 20].

In this paper, we focus on investigating privacy concerns of bystanders, their expectations, and willingness to share data in owners' smart homes. Meanwhile, we equally consider owners' perspectives on bystanders' privacy, owners' understanding of their data practices, and their willingness to address bystanders' privacy. Our work emphasizes the importance of having both per-

*Corresponding Author: Ahmed Alshehri: Colorado School of Mines, E-mail: alshehri@mines.edu
Joseph Spielman: Colorado School of Mines, E-mail: jspielman@mines.edu
Amiya Prasad: Colorado School of Mines, E-mail: amiyaprasad@mines.edu
*Corresponding Author: Chuan Yue: Colorado School of Mines, E-mail: chuanyue@mines.edu

spectives, so that we can better support the privacy protection and the utility of the devices in smart homes.

We design a survey study to understand both owners' and bystanders' perspectives, needs, and willingness to negotiate when it comes to privacy in smart homes. We recruit 300 participants on Amazon Mechanical Turk (AMT) [48] and assign them into two main groups: 200 owners and 100 bystanders. Specifically, we explore the following research questions:

- RQ1: How do owners of smart homes view bystanders' privacy?
- RQ2: What are the concerns, expectations, and needs of bystanders in other people's smart homes?
- RQ3: What are negotiable about data practices in smart homes for owners and bystanders?

To answer RQ1, we asked owners about (1) whether they recognize bystanders' privacy rights, (2) their understanding of their own data practices, and (3) their willingness to address bystanders' privacy. If owners do not recognize bystanders' privacy, they might not be willing to compromise the utility of their devices to address bystanders' privacy concerns. If owners do not understand their own data practices, they might not be able to explain to bystanders what the data practices are. We found that 55% of owners recognize that bystanders have privacy rights in owners' smart homes, 80% of owners would not disclose to bystanders what types of data would be collected, 70% of owners have only either partial understating of their own smart home data practices or no understanding at all, and 73% of owners are willing to address privacy concerns of family members and friends more than those of strangers. We present and discuss these findings in Section 4.1.

To answer RQ2, we asked bystanders about (1) their privacy concerns in other people's smart homes, (2) whether they expect owners to disclose the data practices in smart homes, and (3) their willingness to share data with owners. If bystanders are not concerned about their privacy, there is no need to ask owners to compromise anything. If bystanders expect owners to disclose, we further explore their preferred methods for disclosures. We found that 72% of bystanders feel concerned about their privacy, 62% of bystanders do not expect owners to disclose their data practices, and 65% of bystanders would be willing to share their data in a trusted owner's smart home with their consent. We present and discuss these findings in Section 4.2.

To answer RQ3, we further asked both owners and bystanders to answer the same set of questions regarding their data practice negotiation preferences. We found that owners and bystanders have some different preferences when negotiating data practices. For example, 90% of owners are willing to negotiate data sharing practices more than data collection and data storage practices. An explanation of this might be that owners want to preserve the utility of their devices while respecting bystanders' privacy. Stopping data collection or storage will severely affect the utility of the smart home devices. On the other hand, 99% of bystanders would like to negotiate both data collection and sharing practices. An explanation of this might be that bystanders hope to prevent potential misuses of their data from the beginning, which is the collection. The preference differences between owners and bystanders are not only about the types of data practices to negotiate, but also the choices within each type of data practice. Nonetheless, the majority of owners and bystander show willingness to negotiate, which is a very positive finding.

Following up the survey, we also analyzed 17 smart home devices and their privacy policies to investigate whether some features are available for owners to disclose their data practices and for bystanders to protect themselves. We found that 15 devices do not mention anything about bystanders' privacy, and two devices only mention that owners need to be considerate about bystanders' privacy. Based on all these findings, we further make several recommendations that researchers and device vendors can consider when building privacy protection tools for owners and bystanders. For example, future research can focus on what to negotiate and how negotiation can be supported.

Our main contributions in this paper include: (1) We explore the privacy concerns of bystanders from the perspectives of both owners and bystanders; (2) We investigate owners' and bystanders' willingness to negotiate data practices in smart homes, and what data practices are negotiable; (3) We provide recommendations to address bystanders' privacy concerns and preserve the utility of owners' smart home devices.

# 2 Background and Related Work

## 2.1 Background

**Smart home devices** are IoT devices that people use in their homes. Some of the uses of smart home devices are for entertainment (e.g., smart TVs, smart speakers or gaming consoles), automation (e.g., smart sprinklers or smart thermostats), or for safety (e.g., smart indoor cameras or smart locks). We refer to the main users

who own and control the smart home devices as **owners**, and anyone else who do not own or control these devices but could be around them temporarily (e.g., visiting family members, friends, or domestic workers such as plumbers) as **bystanders**. There are other types of bystanders such as neighbors who do not enter a house and people who live in a house but are more than visitors (i.e., secondary users explained in Section 2.2.1); they are not explicitly included in our study.

**Data practices** we consider in this paper are in three categories: data collection, data storage, and data sharing. For example, the types of data and the frequency of the collection are some data collection practices. The location of the data storage, the retention policies, and the encryption of the stored data are some data storage practices. Last, data sharing practices include how data are shared, for what purposes, and with whom. In this paper, we use data practices to refer to all these three categories of practices.

## 2.2 Related Work

### 2.2.1 Privacy in Smart Homes

Past research on smart home devices has mainly focused on privacy and security issues of owners, who are usually the primary users of the devices [20, 27, 28, 36, 44, 46, 47]. Researchers used methods such as surveys, interviews, and focus groups to investigate owners' perspectives on privacy and security issues in their smart homes. An interesting finding about many owners is that they tended to trust smart home manufacturers, and their preferences for automation or entertainment often influenced their privacy preferences [47]. Further, many owners did not understand the privacy risks associated with the data collected by smart home devices [20, 28]. Owners were somehow aware of the level of privacy invasion smart home devices could have in their homes, but were willing to trade privacy for the utility of the smart home devices [38]. Owners in prior research were considered to have the complete control over their smart home devices. However, when bystanders are present in the smart homes, it becomes an involved problem. Smart home devices can pose risk to bystanders when bystanders have no knowledge of devices or even their existence [43]. Thus, understanding perspectives of bystanders regarding privacy concerns is important, but it was missing in these prior studies.

Some researchers began to mainly study bystanders' privacy in smart homes [7, 11, 33, 43]. Yao et al. concluded through group interviews that bystanders' perceptions on devices revolved around perceived trust, perceived device utility, social relationships, and length of stay [43]. Ahmad et. al. found that some bystanders were uncertain whether smart home devices collect data about them or not, which might inhibit bystanders from making informed decisions about their privacy [7]. Marky et al. investigated how tech-savvy people would like to receive notices of the smart home device existence, and investigated what types of control would be beneficial. They found that visitors would feel more comfortable sharing their data with owners of smart homes if they trusted them in a familiar environment [33]. Bernd et. al. conducted a case study about nannies in smart homes and focused mainly on exploring the socioeconomic power between nannies and their employers in the employers' smart homes [11]. A smart home in this case is seen as a workplace, rather than a personal living space. These studies focused primarily on qualitatively analyzing bystanders' perspectives in smart homes. However, they did not include owners' perspectives of bystanders' privacy. Owners' perspectives would greatly help find a middle ground in terms of having privacy protections for bystanders and preserving the utility of the smart home devices for owners. In this paper, we investigate owners' perspectives and their willingness to negotiate data practices with bystanders.

Researchers in [16, 32, 34] considered the perspectives of owners and bystanders (hosts and guests in an Airbnb environment [1]). Mare et al. aimed at understanding the typical devices that hosts use, devices that guests prefer to use, and reasons why guests would be comfortable with some devices [32]. However, an Airbnb setting is different from normal smart homes in three ways: (1) Airbnb requires hosts to disclose certain devices such as indoor cameras, (2) Airbnb hosts and guests typically do not stay together in the same house, and (3) hosts and guests often do not have established trust as they are strangers to each others. Marky et al. explored privacy perspectives of owners and bystanders in smart homes [34]. However, in their study, owners' perspectives are about their own privacy when bystanders exist in the smart home. They found that owners and bystanders are concerned about their privacy from each other. They conducted qualitative analysis of 42 young adults while we conduct qualitative and quantitative analysis of a larger number of participants. Furthermore, our work differs from theirs because we explore owners' perspective on bystanders' privacy.

Cobb et al. defined contexts that would make users incidental (which is the same as our definition of by-

standers), and studied what context and concerns were bothersome for bystanders [16]. Their study allowed owners and bystanders to answer all the questions from both perspectives. They found that bystanders felt uncomfortable owning smart devices, and owners would turn devices off for bystanders if reasonable justifications were presented. They only considered data collection as a form of accommodations by owners to bystanders' privacy preferences, while we consider the willingness of owners and bystanders to negotiate all three types of data practices and negotiable privacy options.

In multi-user smart homes, unique privacy and usability concerns also arise due to the power unbalance between main users (i.e., owners) and secondary users [22]. Secondary users might not have full control over the smart home devices, but they could still use them and their data will be collected. Researchers have investigated this particular dynamic in [10, 22, 26, 39, 40, 45]. For example, Geeng et al. studied what privacy and usability tensions arose between multiple people in multi-user smart homes and how current designs of smart home devices were unable to properly mitigate or settle the tensions [22]; Koshy et al. found that different needs between pilots (i.e., main users) and passengers (i.e., secondary users) exist, and investigated ways to empower passengers in smart homes [26]. Our focus differs from this group of studies in three aspects. First, secondary users might participate in the decision of buying smart home devices and be considered co-owners. Second, people who live in the same smart home are more likely to perceive the benefits of these devices. This could result in an acceptable trade-off between privacy and utility as found in [47]. Third, the recommendations in these studies are not about negotiation between people, but rather about ways for devices to have additional features to involve secondary users in controlling smart home devices. Our recommendations focus on helping owners and bystanders to negotiate data practices.

#### 2.2.2 Interdependent Privacy

Interdependent privacy means that the privacy of individuals depends on the actions of others. Biczok et al. explored the existence of interdependent privacy in real applications, and found that third-party applications on Facebook violated the privacy of app users' family members and friends [12]. Symeonidis et al. studied the collateral damage of third-party applications on Facebook and found similar results [37]. They also found that participants were concerned about collateral damage because of the lack of transparency and control. The privacy of bystanders studied in our paper is similar to the concept of interdependent privacy. When bystanders enter smart homes, their privacy is dependent on the actions of owners. However, the setting of Online Social Networks (OSNs) is different from the intimate setting of smart homes. Personal data in smart homes can be collected passively without users' actions. Also, the utility of using smart home devices is perceived differently from the utility of using OSNs. For example, posting information in OSNs might be voluntary while collecting data in smart homes might be essential for safety.

Some researchers have looked at the legal consequences of violating interdependent privacy. Symeonidis et al. found that Facebook users might be considered amateur controllers if they share data about others but unlikely to be held accountable [37]. Other researchers summarized that current regulations and policies are inadequate to protect against interdependent privacy violations, and argued that regulations need to explicitly consider interdependent privacy [23, 24]. We argue that regulations targeted on protecting interdependent privacy are applicable to privacy of bystanders. For example, owners of smart homes can be considered amateur controllers of the collected data [41]. Cherubini et al. investigated the multi-party privacy conflicts and proposed dissuasive mechanisms to deter data owners from sharing data about other people without their consent [14]. They found that if platforms or data subjects threaten legal consequences to owners, owners would rethink before sharing. Some news articles argued that smart home owners may violate regulations such as wiretapping laws if they share data about bystanders [4].

## 3 Design of the Survey Study

To answer our three research questions (Section 1), we design a survey study regarding both owners' and bystanders' perspectives, needs, and willingness to negotiate when it comes to privacy in smart homes. We recruit 300 adult participants (200 owners and 100 bystanders) on Amazon Mechanical Turk (AMT) [48]. Our study received the IRB approval, we obtained the informed consent from all participants to take part in the study.

### 3.1 Survey Questions

We conducted our survey on AMT, which is a popular crowdsourcing platform that researchers use for user studies. Figure 1 shows the sets of survey questions for us to derive relevant insights. We have two versions

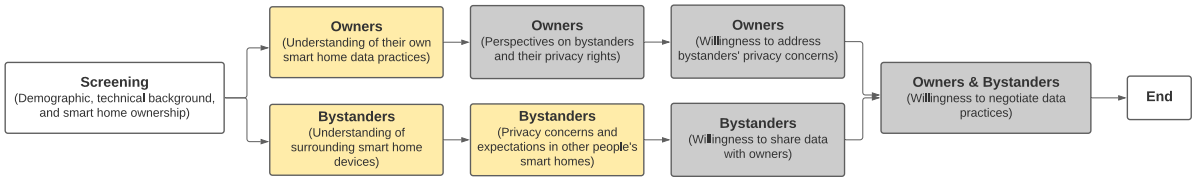


**Fig. (1)** Sets of survey questions to derive relevant insights. The gray rectangles contain questions that are unique to our study. The yellow rectangles contain questions that are partially unique to our study as other researchers have explored some of them.

of the survey. Owners' survey is in Appendix A. Bystanders' survey is in Appendix B. Both surveys contained close-ended questions and open-ended questions. Based on the answer to Q4-7 in Appendix D (Screening and Demographic Questions) regarding whether a participant owns smart home devices, each participant is automatically assigned to the appropriate survey.

Participants who did not own smart home devices were assigned only to answer the bystanders' survey. Participants who owned smart home devices were assigned only to answer the owners' survey, although they could be bystanders too. They do not answer the bystanders' survey because we are mainly interested in the opinions of those bystanders who never owned or controlled smart home devices yet. In other words, the bystanders that we considered are limited to this group of bystanders. This method of assigning participants to different surveys is similar to that in [32, 34].

For owners, we first asked about some demographics and their technical background. Second, we asked general questions about smart homes. Third, we asked owners about their understanding of their own data practices. Fourth, we asked about owners' perspectives on bystanders' privacy. Fifth, we asked owners regarding their willingness to address bystanders' privacy concerns; in this set, we have two questions with different social relationships assumed by mentioning a bystander as a family member or a domestic worker. Last, we asked a set of questions as in Appendix C about what could be negotiable in terms of data practices.

For bystanders, the first two sets of questions are similar to the owners' version of the survey. In the third set, we asked about bystanders' expectations of disclosures from owner. Fourth, we asked bystanders about their notification preferences and the types of data they consider as sensitive. The fifth set of the questions are about bystanders' willingness to share data about them with owners. Social relationship is not assumed in any question of these five sets except that we mentioned "Owners of smart homes can be your friends, family members, or strangers" before the first set of questions. We are interested in a general perspective of bystanders' feelings and expectations. Last, we asked the same set of questions as in Appendix C about what could be negotiable in terms of data practices.

With every close-ended question, a corresponding open-ended question is asked to participants. This approach allows us to better understand participants' reasons for selecting certain answer options for the close-ended questions. We also consider participants' answers to our open-ended questions as a quality control because we explicitly asked them to write two relevant sentences at least. It is worth noting that we mainly focus on the interactions between owners of smart home devices and bystanders because owners often have some control over their devices such as turning off data collection or storing data locally. Meanwhile, no social relationship is assumed in that same set of questions to owners and bystanders about negotiating data practices. In addition, no manufacturers are mentioned in any question. In other words, we do not explicitly prime who would use the data. Also note that different smart home devices (e.g., smart cameras vs. smart TV) can raise different privacy concerns. However, our survey does not ask questions for any specific type of devices because our focus is on the general perspectives on bystanders' privacy from both owners and bystanders.

## 3.2 Participant Recruitment

We designed our study to be comprehensive in terms of acquiring both owners' and bystanders' perspectives. We recruited 300 participants in total: 200 owners and 100 bystanders. Having more owners than bystanders in our study is beneficial to measure owners' perspectives on bystanders' privacy, willingness to negotiate, and privacy preferences. Meanwhile, this owner to bystander ratio is roughly consistent with the smart home device adoption ratio we introduced in Section 1.

Note that initially 325 participants responded to our survey. After eliminating low quality responses, we had 300 participants. We considered any response low quality if it is too short, irrelevant, or repeated by the same participant to multiple questions. A response is too short if it is just one word to an open-ended ques-

tion where we explicitly asked participants to write two sentences at least. We only discarded responses if low quality answers were found more than twice for a participant. We compensated each participant with three U.S. dollars. Note that the federal minimum wage in the U.S. for an hour is $7.25 per hour and the average duration to complete our survey is 17 minutes.

Participants in our study are various in regards to gender, education, age, and technical backgrounds. Table 1 shows a summary of the demographic of our participants. Meanwhile, 85% of the 200 owners have owned their first smart home device for three months at least. Their familiarity with smart homes is helpful in answering our survey. About 83% of owners stated that they owned smart home devices for safety or entertainment. On the other hand, 82% of the 100 bystanders have been to a smart home. This experience is also helpful for them to realistically answer our survey. The rest of bystanders might have answered some of our questions hypothetically since they had not been to a smart home before taking our survey. This can be good in gaining more representative perspectives even from people who have not been exposed to smart homes. Also, 20%, 20%, and 60% of participants reported being tech-savvy, not tech-savvy at all, and in the middle, respectively.

**Table (1)** Demographic breakdown of our participants. The percentages that are not in parentheses are from our study. We also report the U.S. average in parentheses according to the estimate report from the census data of 2020 [5].

| Gender | Age | Education |
|---|---|---|
| Male 64% (49%) | 18-25 10% (13%) | High school or equivalent degree 20% (15%) |
| Female 34% (51%) | 26-40 62% (20%) | Bachelor degree 60% (49%) |
| Other answers 2% (N/A) | 41-60 24% (25%) | Graduate degree 16% (25%) |
| | Over 60 4% (17%) | |

## 3.3 Methodology for Result Analysis

For close-ended questions, we quantitatively analyzed the responses by reporting answer distributions, within-subjects comparisons supported by statistical testing, or between-subjects comparisons supported by statistical testing. We considered a significance threshold of less than 0.05 for statistical testing.

For open-ended questions, we took a bottom up qualitative approach to analyze the responses. We started by familiarizing ourselves with the responses via quickly reading through the responses and looking for common themes. Then, two researchers independently read all the responses from the survey and generated a list of themes based on the Thematic Analysis [13]. First, we generated all the codes at the same level without any hierarchy. Then, we combined similar codes into themes. After that, both researchers met to finalize the themes into a shared codebook (Appendix E) with two main categories: owners and bystanders. It contains eight structural codes (based on our research questions), further divided into more than 75 subcodes. Then, each response was independently coded by researchers. After all responses were coded, the two researchers resolved disagreements resulting from human errors or misunderstanding. Last, a third researcher who was not involved in the coding calculated the inter-coder agreement. Cohen's Kappa, a measure of the inter-coder agreement [21], is 90% , and note that any value larger than 81% is typically considered as excellent.

# 4 Findings

We now present the findings of our survey study. First, we present the findings from owners. Second, we present the findings from bystanders. Lastly, we present what are negotiable for owners and bystanders, and where they can agree in terms of data practices. For open-ended questions, we report the major themes that we found in responses; when the coders analyzed the responses, they highlighted the themes based on the commonality and expressiveness of the responses. We also quote some responses from participants. We refer to owners as O1 to O200 and bystanders as B1 to B100.

## 4.1 Findings from Owners

This subsection answers our first research question (i.e., RQ1 in Section 1). We found from the owners' responses to the survey questions that most of them recognize the privacy rights of bystanders, do not fully understand their own data practices, and are willing to address the privacy concerns of trusted bystanders. The findings are based on the responses to the owners' survey in Appendix A. All the percentages presented in this subsection are derived from the owner participants (n=200).

### 4.1.1 Owners' Perspectives About Bystanders' Privacy

Although some prior studies focused on bystanders' privacy in smart homes, they lacked owners' perspectives on bystanders [7, 43]. Understanding owners' perspectives is essential in making smart homes privacy-preserving as owners are the decision makers when it comes to changing data practices in their smart homes. In our study, we analyzed owners' perspectives on bystanders' privacy as well as the reasons behind them.

In response to Q1-1 and Q1-2, 35% of owners agreed or strongly agreed with "visitors have no privacy rights in my smart home". Some owners thought that the fact that bystanders are only in the smart home temporarily should not give them equal privacy rights. Interestingly, our question was simply about whether bystanders are perceived by owners to have privacy rights in general, not whether they should have equal privacy rights. If owners do not believe that bystanders should have privacy rights, this would limit the effectiveness of any privacy protection. One response is *"Because it's my device they're choosing to use. Because they should not be entering sensitive info at all."* (O22). This participant's response makes sense for active smart home devices with which bystanders need to interact to have their data collected. However, there also exist passive smart home devices such as smart cameras that collect bystanders' data without any interactions.

Note that 45% of owners disagreed or strongly disagreed with the statement in Q1-1, meaning that they recognized bystanders' privacy rights. Some examples are: *"I believe visitors have privacy rights. This is because them using the devices will have their data collected."* (O28), *"I think visitors have the right to request such devices to be turned off, within reason."* (O27) , and *"I think everyone has the right to privacy. I think that it is my responsibility to let my visitors know what kind of privacy they have in my home."* (O55).

It is worth noting that owners who owned their smart home devices longer than three months recognize bystanders' privacy rights more than owners with less than three months' experience. This difference is statistically significant (by using the Wilcoxon Rank Sum Test, the null hypothesis that these two groups of owners do not differ on their responses is rejected; p-value=0.04). We also acknowledge that Q1-1 might have been confusing to some owners in our study. We meant to ask about legal rights, but we did not make it clear. Some owners might have understood the question as if we were asking for human rights rather than legal privacy rights. Future research may want to make it clear in the survey questions.

In regard to the responses to our questions on whether owners would disclose data practices to bystanders: in Q1-3, 42% of owners would disclose the existence of smart home devices to bystanders, and in Q1-4, only 21% of owners anticipate to disclose the types of the collected data to bystanders. There are several reasons why owners would not consider such data disclosures as important. In response to Q1-5, 25% of owners thought of data disclosures to bystanders as unnecessary or unneeded. The argument that many owners made was that bystanders never asked to be informed. Some examples are: *"I would not explain it because I would think it is obvious. Also, I think it would be strange to bring up."* (O34) ,*"If they are not asking about it, I would assume that they do not really care what the device is doing."* (O40), and "*I do not really think they would think of this when visiting. And I will not force them to go through anything that I am not comfortable with myself.*" (O70).

About 24% of owners mentioned that they did not want to make their visitors uncomfortable by discussing data practices. Some of the owners' responses to Q1-5 are: *"I would not go out of my way to tell my visitors. I think it would make them feel uncomfortable."* (O90), *"I think if it were gathering data about folks, a lot of them would be relatively freaked out by the idea. That could influence me to not tell them."* (O66), and *"Well, I think that is kind of too much, it can be mentioned and if the guest has a concern they will surely speak up. This kind of notification would bring paranoia, worry, stress!"* (O63). The thought that bystanders might feel uncomfortable should not stop owners from disclosing. Bystanders would feel betrayed if they become aware of data collection about them without their consent. We discuss bystanders' expectations in the findings from bystanders in Section 4.2.

About 33% of owners mentioned that their lack of understanding of their own smart home data practices might prevent them from disclosing data practices to bystanders. For instance, *"Honestly, I'm not completely sure myself what data is being collected so I would not know what to say. I also don't want to alarm them or deter them from coming to my home."* (O105) and *"I would not explain the types of data that are being collected about them because I myself don't know what types of data is being collected."* (O3) are two responses.

#### 4.1.2 Owners' Understanding of Their Own Smart Home Data Practices

If owners are not able to understand their own smart home data practices, they might not be able to disclose their data practices to bystanders. Thus, measuring owners' understanding is essential in helping make smart homes privacy-preserving for bystanders.

Regarding Q1-6, 10% of owners responded saying they do not understand their data practices at all, while 60% of owners answered that they only partially understand their data practices for a few major reasons, which they gave in Q1-7. Examples include lengthy and complicated privacy policies, the legal and technical lan-

guage of the policies, and the lack of incentives for smart home vendors to simplify their privacy policies. Aligning with our findings, an article in the New York Times examined 150 privacy policies and found that the average time to read an entire privacy policy is 18 minutes [30]. These policies may sometimes have updates so reading them with every update is time consuming.

We asked owners what would help them better understand their own smart home data practices in Q1-8. Owners shared a variety of methods such as concise privacy policies, responsive customer services, easier privacy settings in the companion apps, and third party analysis of smart home devices. One response is *"Maybe watching a video would help. A third party so they would not sugar coat anything."* (O5). Owners also might reach out for help understanding some data practices about their smart homes. Almost half of the owners would ask either a trusted family member or a friend to explain some of the data practices. Consulting experts to understand smart home privacy is a known approach but it is uncommon. Hibshi et. al. suggested in their work that summarizing the privacy and security policies into labels for users would be beneficial [19].

In response to Q1-9, only half of owners have used controlling features, e.g., to delete or modify collected data. The other half either did not know how to use controlling features or never needed to. In Q1-10, we found that among the owners who did not know how to use controlling features, 15% of them found the features difficult to use. Some owners in Q1-11 shared their opinions about controlling features and potential improvements: *"Having a simple and easy to follow interface. Having a user manual guide."* (O20) and *"I have found that these features are hidden deep within settings. Easier access would make it simpler."* (O48). Although the majority of owners thought using the controlling features is not hard, we think it would be useful to improve their existing interface and design. The ability of owners to use controlling features is a sign of at least minimum awareness of their data practices. We explored (by using Chi-Square Test for Association) the relationships between the usage of controlling features by owners (i.e., whether owners use controlling features) and owners' disclosures of devices existence (Q1-3) as well as the disclosures of data types (Q1-4), respectively. We found both relationships to be statistically significant (the null hypothesis that an association relationship does not exist is rejected with p-value=0.02 and p-value=0.01, respectively).

In addition, it is worth noting that owners who owned their smart home devices longer than three months understand their own data practices better than owners with less than three months' experience. This difference is statistically significant (by using the Wilcoxon Rank Sum Test, the null hypothesis that these two groups of owners do not differ on their responses is rejected; p-value=0.0002).

From Q1-12, we found that 87% of owners do not know of any regulations or laws that would require them to disclose privacy practices to bystanders. Some news articles argue that smart home owners might be violating privacy regulations such as wiretapping laws [15]. That article concluded that owners might be safe if the collected data about bystanders are not used. Q1-13 asked owners whether they would be able to concisely write their data disclosure statement if required by law. Half of owners said they would not be able to write such disclosure statements. They would turn to the Internet to get help if needed. Interestingly, owners expect smart home device manufacturers to have some templates for them to use when disclosing privacy practices to bystanders. Two examples are: *"I could contact smart device agent for support. I can also check the internet for direction."* (O80), and *"looking disclosure statements up online and downloading templates. I would also seek disclosure info on the official websites, while logged into my account"* (O111). In reality, smart home manufacturers do not even consider bystanders in their privacy policies, so providing templates for owners is currently unlikely. Section 5.1 discusses this in details.

#### 4.1.3 Owners' Willingness to Address Concerns

We examine the willingness of owners to address bystanders' privacy concerns in this subsection with the main results shown in Figure 2. First, we asked in Q1-15 about if owners have any deal breakers about stopping the collecting of some types of data. We found that 73% of owners would stop collecting any types of data in general if their visitors were uncomfortable. It is likely that owners may have different interpretations of their guests. To avoid some potential confusion, we explicitly asked scenario-based questions about two different types of visitors or bystanders: trusted bystanders (e.g., family members or friends) and untrusted bystanders (e.g., domestic workers such as plumbers).

Based on the responses to Q1-17, 70% of owners are willing to address privacy concerns of their family members. However, when we asked about the same scenario for domestic workers in Q1-18, only 51% of owners are willing to address domestic workers' privacy concerns. We explored (by using the McNemar's Test) the association between owners' willingness to address privacy con-

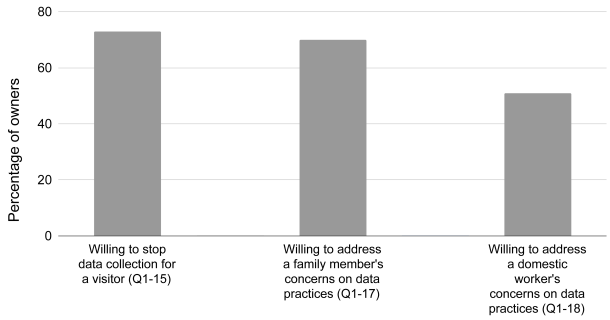


**Fig. (2)** Owners' willingness to address concerns.

cerns and their social relationship with bystanders. We found the association to be statistically significant (the null hypothesis that an association relationship does not exist is rejected with p-value=0.015.)

In Q1-19, we asked participants to explain their answers to the previous two questions. About 17% of owners do not care about bystanders' privacy: *"Because I might care about some family. I would not care at all about a worker I was paying to be there."* (O89), and *"A family member would get special consideration and I would most certainly turn the device off. A domestic worker getting uncomfortable about a smart device would give me pause as to why they do not want to be monitored, and they would need a good reason for me to disable the device instead of just finding another domestic worker."* (O79).

About 40% of owners consider safety as important when having domestic workers in their homes so they seem to be less willing to negotiate about what data to be collected in their homes: *"I value my family and want to make sure they're comfortable. I trust them and respect them. While I respect domestic workers, I will keep devices on for my own safety. I am a small woman and can be easily overpowered. It also protects me against potential theft or damage."* (O131), and *"Again, if it is a domestic worker, I will not disable anything at all for my own safety. Cameras are in place to protect me. They can leave if uncomfortable. I only apply this to strangers."* (O100). In short, some owners are willing to negotiate data practices when the utility of their devices is not compromised and when they trust bystanders.

## 4.2 Findings from Bystanders

We answer our second research question (i.e., RQ2) in this subsection. We found that most bystanders are concerned about their privacy in other people's smart homes, and would not expect owners to disclose data practices. Bystanders also would be willing to share data about them with owners of smart homes if their privacy concerns are addressed, they trust the owners, and they give consent regarding their data. The findings are based on the responses to the bystanders' survey in Appendix B. All the percentages presented in this subsection are derived from the bystander participants (n=100).

### 4.2.1 Bystanders' Concerns in Smart Homes

In response to Q2-1 where we asked bystanders about their concerns while visiting other people's smart homes, 72% of bystanders feel uncomfortable or vulnerable about their data being collected in other people's smart homes. A major reason for the discomfort is the lack of control for bystanders over their data: *"It makes me kind of uncomfortable for device to be collecting data on me. Since these would not even be my devices and I really would not even know how my data was being used."* (B12), *"Uncomfortable, I do not like not being able to control what data is being taken."* (B66), and *"I feel pretty anxious about it because I do not feel like I have any control over the information being collected."* (B32). Another reason for the discomfort is not asking bystanders for consent about collecting their data: *"I would feel unsafe due to the fact that the devices are not asking for my permission to collect my data."*(B14), *"I feel offended for not getting my permission."* (B50), and *"I don't want my data to be collected by other without permission."* (B80). About 24% of bystanders feel uncomfortable only about the collection of some types of data: *"I am uncomfortable with some types of data collection, such as storing voice recordings when the device is not in use. However, data that is non-identifying or otherwise does not impact personal privacy I am okay with."* (B04), and *"It depends on the type of data. If it is personal or identifiable things, I would feel uncomfortable and nervous."* (B78).

Among the bystanders who feel vulnerable, 40% of them consider the collection of their data in other people's smart homes as a violation of their privacy. Some examples are: *"Because it is common courtesy to let other people know when you are recording them. In some states, including the one where I live, it is also illegal to record people without getting their consent."* (B29), *"I would feel like my privacy had been violated if I found out the device collected data on me."* (B72), and *"I would not like the fact that it is violating my privacy without my consent."* (B90). Note that wiretapping laws are enforced by the federal government and individual states in the United States [4]. The federal laws require a one-party consent to capture any recording of other people, and some states require a one-party consent while some others require a two-party consent [4, 15].

About 27% of bystanders felt indifferent about the collection of their data. Among them, 40% consider that they do not have privacy rights in other people's smart homes, 32% feel helpless as everything collects data, and 28% accept the trade-off for the features that would be available in exchange of their data.

#### 4.2.2 Bystanders' Expectations of Privacy in Other People's Smart Homes

We asked bystanders whether they expect owners to disclose their data practices or not in Q2-2 and Q2-3. About 62% of bystanders do not expect (i.e., anticipate) owners of smart homes to inform them about owners' data practices for a few reasons. About 72% of bystanders who do not expect owners to tell them about data practices consider that owners may not be aware of their own smart home data practices. As a result, they would not be able to inform bystanders about their data practices. Some responses are: *"To be honest, I'd be shocked if owners knew all of the particulars. If they bother to read any of it at all, people tend to skim over these things, just as they often do with smartphone apps."* (B68), *"I don't think most people even know themselves, even if they are the owners of the devices."* (B86), and *"I think that most owners do not know about what data is taken. I think they would not be able to explain it to me."* (B49). Our findings from owners (Section 4.1) align with these bystanders' perspectives of owners' inability to understand their own data practices. This inability of owners may affect the disclosure of their data practices to bystanders.

About 10% of bystanders do not expect owners to disclose data practices as it is not seen as a norm in a visit: *"Because it is not something that is normally discussed."* (B08), and *"It would be nice if they told you when they are on. But it makes for a weird social interaction."* (B51). Some other bystanders do not see the disclosure as owners' obligation since that is their house and their rules: *"I do not expect them to tell me because it is their own home. I can be curious and ask but I do not expect them to tell me without asking."* (B16), and *"I do not expect them to tell me because it is their property and they do not need to tell me anything."* (B26).

On the other hand, 38% of bystanders expect owners to disclose smart home data practices. Owners can show respect by doing so: *"If my data is being gathered and stored in their devices I want to know, I do not feel it is right to collect data when you are not aware it is being collected."* (B25), and *"I have a right to know. My privacy should be respected."* (B80). Meanwhile, many bystanders think owners are obligated to disclose: *"Anytime someone or something is collecting my personal data I have a right to know."* (B78).

About 15% of bystanders think that most owners are careless about their data. As a result, owners would not worry about bystanders' data: *"if they have a smart home, they are not worried about this, let alone about the data of others being collected."* (B22). This sounds convincing; however, the studies in [8, 31] show that owners worry about bystanders' data more than their own data. It could be for preventing legal liabilities.

Among bystanders who expect owners to disclose, 40% of them would feel betrayed if they are not informed by owners about data practices: *"I would expect them to tell me to be careful. If they respect me enough to let me enter, then they would respect me enough to tell me about the data practices."* (B38), and *"If someone had a device that was collecting data about me without telling me I would feel that my privacy had been violated. It would seem dishonest to me if they did not tell me, and kind of creepy."* (B21). This finding is similar to the findings in [7, 11, 34, 43]. In our finding, we noticed that a bystander's relationship with an owner plays a role in the bystanders' feeling of betrayal: *"It makes me feel uncomfortable, like I'm being spied on in my own friend's home."* (B70), and *"I do not really care that much if it is somewhere I do not spend a lot of time. Maybe it would be different if it was at a girlfriend's or something."* (B96). The expectations change as the relationship with the owner changes.

We also explored (by using Chi-Square Test for Association) the relationships between bystanders' exposure to smart homes (i.e., whether they have been to a smart home before) and their privacy concerns (Q2-1) as well as expectations (Q2-2), respectively. We did not find either of the two relationships to be statistically significant (the null hypothesis that an association relationship does not exist cannot be rejected with p-value=0.31 and p-value=0.59, respectively).

#### 4.2.3 Bystanders' Sensitivity to Data Types

In response to Q2-4, 90% of bystanders consider video footage and pictures about them as most sensitive. For example, some participants' responses show the sensitivity towards capturing their faces: *"Because I do not want my features to be recorded. I particularly do not want my face to be captured."* (B82), and *"If something is recording my face or word for word what I am saying it needs to be known"* (B22). Facial data are critical as modern smartphones and security systems use fa-

cial recognition mechanisms to authenticate users. This might increase the sensitivity of collecting facial data about bystanders. In addition, 65% of bystanders consider audio recordings as sensitive. Previous work such as [16, 33] also found that bystanders feel more concerned about data collection by smart cameras or smart speakers than some other smart home devices.

Smart home devices could be connected to an automation platform such as Alexa, Google Home, or IFTTT (If This Then That) services [3]. For example, a smart camera might be programmed through IFTTT to post a picture (to Twitter or Facebook) of the living room at noon everyday. If a bystander happens to be at the owner's smart home at noon, the bystander's picture could be posted publicly. It is worth noting that considering the automation of smart homes adds more complexity to reaching an agreement between bystanders and owners as the automation websites or services usually have their own privacy policies. A solution should then consider the devices' privacy policies, owners' privacy policies, and the automation policies. In response to Q1-2, 43% of owners use automation services. Future privacy protections need to consider that. Researchers should consider turning some data collections off or improving the automation rules to protect bystanders' privacy and still preserve the utility of the devices.

#### 4.2.4 Bystanders' Preferences to Receive Notifications About Data Practices

We asked bystanders in Q2-5 about their preferences in receiving notifications about different types of data practices in other people's smart homes. About 85%, 77%, and 60% of bystanders want about collection, sharing, and storage of the data, respectively. Then, we asked bystanders about how they would like to be informed in Q2-6 and Q2-7. Bystanders prefer to be informed about data practices in two major ways. One is by the owners themselves, either verbally, via a digital means, or via a written notice. The other is through the smart home device manufacturers. For example, smart home devices' privacy policies and related documents should have some information about bystanders' data.

In more details, 80% of bystanders prefer to be told about smart home data practices by owners themselves. The fact that owners would have access to the collected data makes this understandable. Among these bystanders, 75% of them prefer to be informed via digital means (e.g., via email, texts, or app notifications). This could help avoid having a conversation with owners about data practices as we mentioned above that

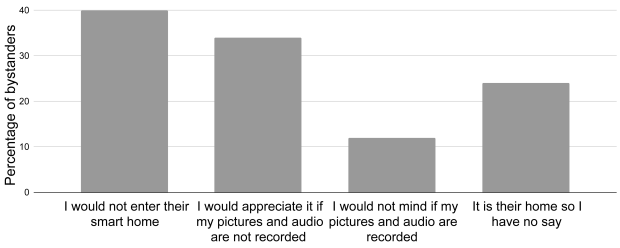


**Fig. (3)** Bystanders' responses to the question Q2-8.

some owners and bystanders consider discussing data practices as awkward and abnormal. Meanwhile, 20% of these bystanders would like to be told about data practices by the smart home devices themselves. The manufacturers may need to design smart home devices with appropriate features so that bystanders could be notified about any data collection. By either owners or devices, bystanders mentioned being told via verbal notices, post-it notes, physical notifications (lights, shutters or others), their smartphones (text, call, or email), and others. For verbal notices, an owner could explain what devices are collecting data, or some devices such as smart speakers could recognize bystanders and deliver a verbal notice. Many bystanders appreciate transparency and being given some control over their data.

The study in [7] emphasizes the importance of improving the design of smart home devices to be more informational to bystanders. This would be ideal if all owners believe that bystanders should have their privacy honored even though that might impact the utility of the smart home devices. However, we found that 35% of smart home owners would not honor bystanders' privacy or would not compromise the utility of their smart home devices. This may push the research community to explore more middle grounds between owners and bystanders instead of focusing entirely on improving privacy tools for one party.

#### 4.2.5 Bystanders' Willingness to Share Their Data with Owners

We asked bystanders what they would do if their privacy concerns were not addressed in Q2-8. As shown in Figure 3, 40% of bystanders would not enter the smart home. Some bystanders may be able to afford leaving someone's smart home, but others (e.g., nannies) may not be able to do so. Bernd et. al. discussed how nannies have privacy concerns but could not address the concerns due to the differences in the power dynamics between parents or owners and nannies [11].

We also asked bystanders what should happen if they have a disagreement regarding the data practices

with owners of smart homes in Q2-9. More than two thirds of bystanders believe that there should be some negotiation about data practices when they are in other people's smart homes. Negotiating data practices means that owners and bystanders would make some compromise to reach an agreement. For example, owners can store data for a shorter time period instead of storing bystanders' data permanently [20].

In Q2-10, we asked bystanders if the technical background of owners would influence their willingness to share data with owners. About 35% of bystanders confirm the influence. Among those bystanders, 79% of them consider (based on their responses to Q2-11) that tech savvy owners have a better understanding of privacy issues. This might affect whether they trust owners' ability to protect their data if collected: *"Even if the homeowner did not know how to access my recorded data it would just make me uncomfortable. Especially if other people might have access."* (B37), and *"I have more trust in someone with technical knowledge to be aware of good data practices. I think they would make better choices about how data is shared and know how to keep it secure."* (B52). Also, tech-savvy owners will likely be able to explain data practices accurately to bystanders, thus helping bystanders make more informed decisions about their data: *"The more tech-savvy smart home owner would be better able to explain what is being collected. They would be able to help me determine if I should enter the house."* (B66), and *"If they have a better technical background then they would know exactly what data was being collected. They would be able to explain it to me, and I would have the opportunity to ask them not to collect the data in certain situations."* (B15). This finding aligns with that from Mare et. al. [32]. They found that some guests have concerns about the capability of hosts to secure their smart home devices, which may lead to the exposures of guests' data or even some risk to their safety in a case of Airbnb.

In addition to the technical background influence, trust also impacts bystanders' willingness to share data as found similarly in [33]. First, trust between bystanders and owners is a factor: *"Depending on the tech-savvy-ness, I might be slightly more concerned about what information they are gathering and what they are doing with it. This would also depend on my relationship with the person."* (B86). Note that while no social relationship is assumed in our questions, some bystanders such as B86 and B96 (shown in Section 4.2.2) indicated certain social relationship assumptions in their responses. Second, trust between bystanders and smart home vendors is also a factor: *"It is the tech companies I do not trust. Regardless of how knowledgeable the homeowner is, I simply do not trust tech companies to be completely honest and transparent with their end users. I believe that anyone who does is being naive."* (B18).

## 4.3 Negotiable Data Practices for Owners and Bystanders

We answer our third research question (i.e., RQ3) in this subsection. We explore what types of data practices could be negotiable for owners of smart homes and bystanders. We are also interested in whether owners and bystanders would choose to negotiate the same privacy options. If they choose the same privacy options from what were identically presented to them in Appendix C, no negotiation would be needed while researchers and device vendors would just need to implement those options. However, we found that most owners and bystanders are willing to negotiate but do not agree on the same set of options. Therefore, further negotiations between owners and bystanders are needed, and researchers or vendors may consider facilitating such negotiations.

The privacy options presented in our survey questions are derived from several previous research studies [7, 20, 28, 31, 36, 43], and our own analysis of what could be possible in a smart home environment. The goal of exploring the negotiability is to explore the willingness to negotiate data practices in order to reach an agreement between owners and bystanders.

Typically, the more privacy preserving for bystanders the smart home is, the lower utility the smart home devices would retain. For example, if an owner turns off a smart camera, this main utility of the camera to increase home safety is defeated. It is clear that when we move towards honoring one party's rights, we may compromise the other party's interests. This makes it obvious why minimizing compromise to each party might result in a better solution for both, and why a negotiation approach could be helpful.

**Negotiation About Data Collection.** In response to Q3-1, 80% of owners are willing to negotiate some data collection practices with bystanders to some extent. We asked the almost identical question to bystanders in Q3-2, 99% of bystanders are willing to negotiate data collection practices with owners to some extent. Owners' most common negotiable privacy option is turning all the devices off, while bystanders' most common negotiable privacy option is turning devices off in some rooms. We asked the open-ended question Q3-3 for owners and bystanders to explain their answers to

Q3-1 and Q3-2, respectively. The responses from one bystander is: *"I would respect their usage of their devices in their home. Though I would want it turned off in private areas like a guest bedroom and bathroom."* (B43). These results show that most bystanders are not greedy about data collection. Figure 4 illustrates the detailed distribution of the negotiable data collection privacy option selections from owners and bystanders. We explored (by using Chi-Square Test for Association) the relationship between the participant type (i.e., owners vs bystanders) and the distribution of the negotiable data collection privacy option selections. We found the relationship to be statistically significant (the null hypothesis that an association relationship does not exist is rejected with p-value=0.0000005).

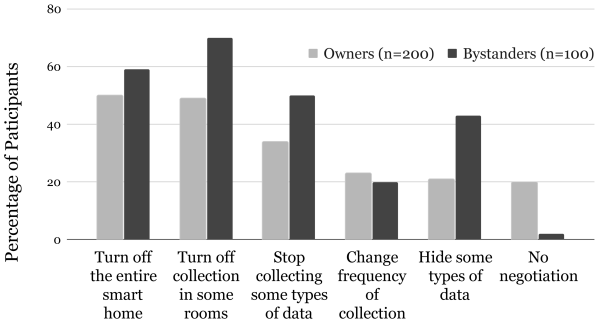


**Fig. (4)** Willingness to negotiate privacy options about data collection. Note that these questions are multiple-answer questions.

**Negotiation About Data Storage**. Regarding Q3-4 and Q3-5, 49% of owners would negotiate temporary storage, and 60% of bystanders would negotiate the same option. This is the common option to both owners and bystanders. The response from one bystander is: *"I think having it stored temporarily is safe for both parties. After a while, i would know my data is not recorded anymore."* (B53). Safe for both parties means, for example, that owners can keep their safety cameras on and bystanders can have the assurance that their data would be deleted. Figure 5 shows the different data storage privacy options that owners and bystanders would negotiate and their corresponding selection percentages. We explored (by using Chi-Square Test for Association) the relationship between the participant type (i.e., owners vs bystanders) and the distribution of the negotiable data storage privacy option selections. We found the relationship to be statistically significant (the null hypothesis that an association relationship does not exist is rejected with p-value=0.000009).

**Negotiation About Sharing Data with Others by Owners**. Practically speaking, owners and bystanders cannot do much to stop companies from sharing their data. With the current regulations, companies are free to process the data as they want if users consent. In response to Q3-7 and Q3-8, 55% of owners would not share data about bystanders, and 65% of bystanders would prefer no sharing at all for their data by owners. From the responses to the open-ended question Q3-9, some bystanders consider the recipient of the shared data to be a factor in their willingness to negotiate with owners. Bystanders would care less if they know with whom the collected data would be shared. Many bystanders also prefer the privacy option "get approval from bystanders". An example response is: *"Sharing with approval is the safest and smartest way in my opinion. Both sides get what they want."* (B76). Owners would get to share data and bystanders would get the transparency and the request for approval from owners. Figure 6 shows the differences between owners and bystanders when negotiating sharing data with others by owners. We explored (by using Chi-Square Test for Association) the relationship between the participant type (i.e., owners vs bystanders) and the distribution of the negotiable data sharing privacy option selections. We found the relationship to be statistically significant (the null hypothesis that an association relationship does not exist is rejected with p-value=0.005).

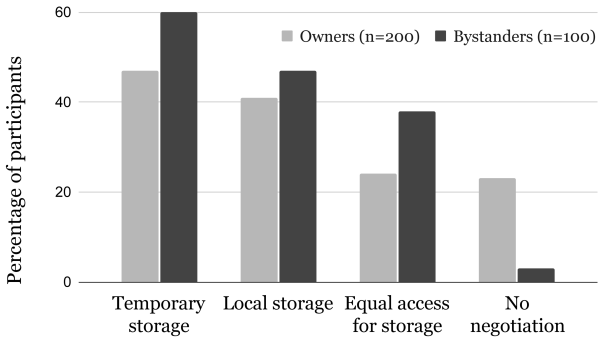


**Fig. (5)** Willingness to negotiate privacy options about data storage. Note that these questions are multiple-answer questions.

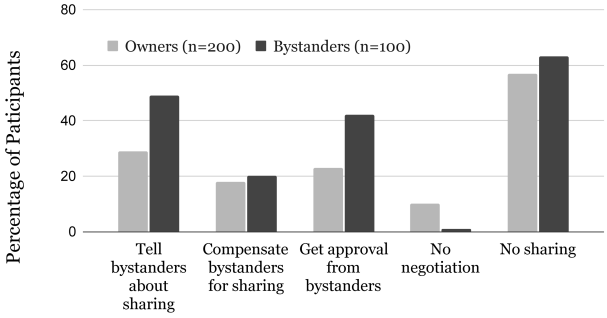


**Fig. (6)** Willingness to negotiate privacy options about data sharing. Note that these questions are multiple-answer questions.

When we compare the three types of data practices, 90% of owners are willing to negotiate data sharing more than negotiating data collection and storage; 99% of bystanders want to negotiate data collection and sharing more than data storage. Owners can to some extent decide not to share data. However, stopping the data collection or not storing collected data will compromise the utility of smart home devices. Also, controlling storage might require some technical background for owners to configure the options we presented in the survey.

### 4.4 Summary of Findings

We now present a summary of the key findings and how they answered our research questions. Regarding RQ1, we found that 55% of owners recognize bystanders' privacy rights in their smart homes. This is promising because if owners do not recognize bystanders' privacy, they might not be willing to address bystanders' privacy concerns. We also found that 80% of owners would not disclose to bystanders regarding what types of data would be collected about them. This shows a need for raising awareness of the importance of data disclosures to bystanders. In our findings, 70% of owners have no understanding or partial understating of their own data practices. If owners do not understand their own data practices, they might not be able to explain to bystanders what the data practices are. In addition, 73% of owners are willing to address privacy concerns of family members and friends more than those of strangers.

Regarding RQ2, we found that 72% of bystanders feel concerned about their privacy. If bystanders are not concerned about their privacy, no need to ask owners to compromise the utility of their devices. We found that 62% of bystanders do not expect owners to disclose their data practices. If bystanders expect owners to disclose, we should explore methods of disclosures. We found that 90% of bystanders consider video footage and pictures as sensitive data. Classifying data into sensitive and insensitive types could help owners preserve the utility of their devices when addressing bystanders' privacy. For example, owners could disclose data practices that collect sensitive data only. Finally, we found that 65% of bystanders would be willing to share data about themselves in an owner's smart home if they consent and trust the owner.

Regarding RQ3, we found that owners and bystanders have different privacy preferences when negotiating data practices. For example, 90% of owners are willing to negotiate data sharing practices more than data collection and storage practices. An explanation of this might be that owners want to preserve the utility of their devices while respecting bystanders' privacy. Stopping data collection or storage has a negative impact on the utility of the smart home devices. On the other hand, bystanders are willing to negotiate both data collection and sharing practices. An explanation of this might be that bystanders want to prevent potential misuses of their data from the beginning, which is the collection of the data. Beyond these differences, but also the preferences within each type of data practice are different between owners and bystanders. Nonetheless, the majority of owners and bystander show willingness to negotiate and that is a promising finding.

## 5 Discussion

In this section,we first analyze and discuss whether bystanders' privacy has already been considered in some current smart home devices. Second, we present our recommendations derived from our findings. Third, we discuss the limitations of this paper.

### 5.1 Current Devices Often Do Not Address Bystanders' Privacy Concerns

We analyzed 17 smart home devices along with their privacy policies and other related documents. These devices include three smart cameras, two smart speakers, two smart switches, and others as listed in Table 2 of Appendix F. We focused on analyzing how these devices deal with the privacy of bystanders, and obtained some useful observations. Based on their features, privacy policies, and other related documents, 15 smart home devices do not mention anything about bystanders' privacy. Only two devices mention bystanders' privacy, but no real assistance to its protection is provided. For example, Ring's smart doorbell privacy policy states that *"You [the owner] are solely responsible for ensuring that you comply with applicable law when you use our products or services"* [49]. Its website goes on to suggest that an owner should display a notice to alert visitors that the owner is using smart home devices that may or may not be taking data that can be used to personally identify them. Similarly, the website of Blink smart cameras sells physical signs as an accessory along with the cameras to warn bystanders of video recordings [2]. However, this idea of putting up a physical sign to alert guests may lead to awkward conversations between bystanders and owners. From our results presented in Section 4, a

third of owners would avoid bringing up anything about privacy that could make their guests paranoid.

There are some existing features that owners could use to protect bystanders' privacy to a certain extent. For example, Alexa has voice commands called skills (with corresponding APIs) to delete listening history such as the command "Alexa, delete everything I said today". Owners can use that to protect bystanders' data. Some companies, like Withings and Omron, allow for eligible customers (those impacted by the Children's Online Privacy Protection Act (COPPA) or the General Data Protection Regulation (GDPR) [50, 51]) to call a service center or email the company to delete selected data. Lastly, Ring has implemented a feature called "Privacy Zones" that can block out certain parts of the camera's field of view. While some of these 17 devices (such as Amazon Echo and Nest thermostat) have features and user interfaces that are supposed to allow for bystanders' interactions, those features normally require a signing-up process that forces a guest to register an account with the manufacturer for additionally sharing the data with third parties. Also, such guest access does not give bystanders the ability to share privacy preferences and enforce them. It would be desirable for smart home vendors to provide features for owners and bystanders to better protect the privacy of bystanders.

## 5.2 Recommendations for Future Smart Home Devices

Privacy features for smart home devices should consider the trust between owners and bystanders. In our findings, 73% of owners are willing to address the privacy concerns of trusted bystanders, and 65% of bystanders are willing to share data with trusted owners. Based on our findings, we present some recommendations for addressing privacy concerns of bystanders while preserving the utility of smart home devices for owners.

### 5.2.1 Owner-Focused Recommendations

**To Better Understand Their Data Practices.** In their responses, owners shared their preferences on what could help them understand their data practices better. They shared a variety of desirable methods to improve their understanding. Smart home vendors could provide short and concise privacy policies, effective and responsive customer services, and straightforward privacy settings in the companion apps. In addition, third party analysis of smart home devices would be helpful.

**To Better Disclose Data Practices to Bystanders.** Ideally, smart home devices should be able to detect bystanders and disclose the data practices to them directly. Owners and bystanders in their responses preferred an indirect method of discussing data practices to avoid awkwardness. After the disclosure, bystanders might share their privacy preferences. The need for empowering bystanders with privacy tools was also found in previous work. For example, Cobb et al. found that 73% of bystanders would like to know about the data collection and have some control over their data in other people's smart homes [16]. Smart home vendors can provide methods for bystanders to share their preferences. If bystanders' privacy preferences conflict with owners' privacy preferences, there should be some negotiation mechanisms for them to resolve the conflicts.

**To Achieve a Balance Between Utility and Privacy.** Any privacy features that aim for protecting bystanders' privacy should consider a balance between that and preserving the utility of the smart home devices. One way to reduce the loss of utility is to enforce the privacy protection temporarily. The default smart home data practices should resume as bystanders leave the smart home. Some owners would not turn devices off because that might jeopardize their safety: *"I would not stop collecting video data. If something happens in my home. no matter the circumstance I would like to have video evidence of what happened"* (O55). To accommodate such owners, we recommend the temporary storage of collected data so that owners could preserve the utility of their devices and bystanders could have assurance about their privacy. In our findings, most owners and bystanders prefer the temporary storage of collected data when negotiating data storage.

### 5.2.2 Bystander-Focused Recommendations

**Notifying Bystanders About Sensitive Data**. About 90% of bystanders in our study consider video recordings and pictures as sensitive. Other data types are seen as less sensitive to bystanders. Smart home vendors should provide tools to directly notify bystanders about data practices, or for owners to do so. Either way, considering notifying bystanders about only sensitive data types would be better because bystanders would avoid being burdened with too many notices. Also, bystanders shared several ways to receive the notifications of data practices. Receiving notifications via a digital means (e.g., a smartphone app, a text message, or an email) is a common option by bystanders. Considering this approach aligns with some owners' desire to avoid discussing data practices with bystanders.

**Negotiating Data Practices.** Ideally, owners and bystanders can have their preferences matched without conflicts. However, this might be hard because owners want to preserve the utility of their devices and bystanders want to protect their privacy. Mediating conflicts between them can be done via negotiation. Owners can have their preferences set, and then bystanders can agree or disagree. If conflicts arise, some rounds to negotiate can be helpful. In addition to our recommendations, future research could investigate new privacy features or tools to better support owners and bystanders with the goal of preserving the utility of smart home devices while protecting bystanders' privacy.

### 5.3 Limitations

First, participants from AMT may not be very representative. Prior research showed that AMT workers are generally tech-savvy and more privacy-conscious than average Americans [25]. Thus, our study likely overestimates both bystanders' privacy concerns and owners' willingness to negotiate data practices with bystanders. Second, self-reported privacy concerns may differ from actual behaviors. Researchers have called this phenomenon "privacy paradox", and they found that participants overestimated their privacy concerns [6, 42]. Our study may be susceptible to this bias, i.e., overestimated participants' privacy concerns. Similarly, relying on participants to self-report their perceived understanding (e.g., of data practices as in Q1-6 and Q1-9) may not always be reliable. Our study may be susceptible to this bias too, e.g., tech-savvy participants may have overestimated their understanding.

Typically, there are at least two types of smart home devices. The first type is passive devices which bystanders do not need to interact with to have their data recorded. The second type is active devices with which bystanders need to interact in order to have their data collected. In this study, we mainly considered the first type, but some owner participants might have considered both types or the second type in answering some of our questions. For example, an owner answered our question regarding whether bystanders should be told about data practices with *"if they (bystanders) do not use it, it does not collect data about them."* (O43). This is true for the second instead of the first type of smart home devices. Future research should clearly state such differences to participants, and also explore how different devices influence participants' answers.

In addition, previous work found that owners might trust some specific manufacturers more than others to protect their privacy [47]. It is likely that devices from different manufacturers might also cause different privacy concerns to bystanders. Meanwhile, we only considered sharing bystanders' data with owners, which is different from sharing with manufacturers and third parties. We did not examine these effects in our work, but they can be investigated in the future research.

## 6 Conclusion

Smart home IoT devices collect data not only from owners of the devices, but also from bystanders in a smart home. Existing research mainly considered the privacy concerns of bystanders from their own perspectives. In this paper, we designed and conducted a survey study to more comprehensively explore the privacy concerns of bystanders from the perspectives of both owners and bystanders. For owners (n=200), we investigated their understanding of their own data practices, their views on bystanders' privacy, and their willingness to negotiate data practices with bystanders. For bystanders (n=100), we investigated their privacy concerns, their expectations of disclosures by owners, and their willingness to share their data with owners.

We found that most owners of smart homes recognize the privacy rights of bystanders, do not fully understand their own data practices, and are willing to address the privacy concerns of trusted bystanders. We found that most bystanders have concerns about their privacy in other people's smart homes, do not expect owners to disclose data practices, and are willing to share their data with owners if asked for consent. We also explored the willingness of owners and bystanders on negotiating data collection, storage, and sharing in smart homes. We found that many owners and bystanders have different preferences regarding negotiating data practices. Based on our findings, we provide some recommendations for enhancing the privacy protection in smart homes. Our study could be helpful for researchers and smart home device vendors to improve privacy protection for bystanders while preserving the utility of smart home devices for owners.

## Acknowledgments

We thank anonymous reviewers for valuable comments. This research was partially supported by funding from Meta and NSF grant OIA-1936968. Ahmed Alshehri is supported by the Islamic University of Madinah.

# References


[1] Airbnb . https://www.airbnb.com/.

[2] Blink Physical Sign . https://www.amazon.com/Blink-Yard-Window-Decals-Bundle/dp/B0711XS1J4.

[3] If This Then That (IFTTT) . https://ifttt.com/.

[4] Laws on Recording Conversations in all 50 states. https://www.mwl-law.com/wp-content/uploads/2018/02/RECORDING-CONVERSATIONS-CHART.pdf.

[5] U.S. Census . https://www.census.gov/library/stories/2020/12/census-bureau-provides-population-estimates-for-independent-evaluation-of-upcoming-census-results.html#:~:text=The%20tabulation%20of%20the%20official,explained%20in%20more%20detail%20below.

[6] Acquisti, A., and Gross, R. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *International workshop on privacy enhancing technologies* (2006).

[7] Ahmad, I., Farzan, R., Kapdia, A., and Lee, A. J. Tangible privacy: Towards user-centric sensor designs for bystander privacy. In *Proceedings of the ACM on Human-Computer Interaction* (2020).

[8] Akter, T., Dosono, B., Ahmed, T., Kapadia, A., and Semaan, B. I am uncomfortable sharing what i can't see: Privacy concerns of the visually impaired with camera based assistive applications. In *Proceedings of 29th USENIX Security Symposium* (2020).

[9] Alarm. Smart home statistics. https//www.alarms.org/smart-home-statistics/.

[10] Apthorpe, N., Mathur, A., Emami-Naeini, P., Chetty, M., and Feamster, N. You, me, and iot: How internet-connected home devices affect interpersonal relationships. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing* (2019), CSCW '19.

[11] Bernd, J., Abu-Salma, R., and Frik, A. Bystanders' privacy: The perspectives of nannies on smart home surveillance. In *Proceedings of the 10th USENIX Workshop on Free and Open Communications on the Internet* (2020).

[12] Biczók, G., and Chia, P. H. Interdependent privacy: Let me share your data. In *International conference on financial cryptography and data security* (2013).

[13] Blandford, A., Furniss, D., and Makri, S. In *Qualitative HCI Research: Going Behind the Scenes* (2016), Morgan & Claypool Publishers.

[14] Cherubini, M., Salehzadeh Niksirat, K., Boldi, M.-O., Keopraseuth, H., Such, J. M., and Huguenin, K. When forcing collaboration is the most sensible choice: Desirability of precautionary and dissuasive mechanisms to manage multiparty privacy conflicts. No. CSCW 2021.

[15] Clauser, G. Security Cameras, Ethics, and the Law. https://www.nytimes.com/wirecutter/blog/security-cameras-ethics-and-the-law/.

[16] Cobb, C., Bhagavatula, S., Garrett, K. A., Hoffman, A., Rao, V., and Bauer, L. "i would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. In *Proceedings on Privacy Enhancing Technologies* (2021).

[17] Das, A., Degeling, M., Smullen, D., and Sadeh, N. Personalized privacy assistants for the internet of things. In *IEEE Pervasive Computing: Special Issue - Securing the IoT* (2018).

[18] Das, A., Degeling, M., Wang, X., Wang, J., Sadeh, N., and Satyanarayanan, M. Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops* (2017).

[19] Emami-Naeini, P., Agarwal, Y., Cranor, L. F., and Hibshi, H. Ask the experts: What should be on an iot privacy and security label? In *proceedings of the 41st IEEE Symposium on Security and Privacy (S&P'20)* (2020).

[20] Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., and Sadeh, N. Privacy expectations and preferences in an iot world. In *Symposium on Usable Privacy and Security (SOUPS)* (2017).

[21] Fleiss, J. L., Levin, B., and Paik, M. C. Statistical methods for rates and proportions. In *John Wiley & Sons* (2013).

[22] Geeng, C., and Roesner, F. Who's in control? interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019).

[23] Humbert, M., Trubert, B., and Huguenin, K. A survey on interdependent privacy. In *ACM Computing Surveys (CSUR)* (2019).

[24] Kamleitner, B., and Mitchell, V. Your data is my data: a framework for addressing interdependent privacy infringements. In *Journal of Public Policy & Marketing* (2019).

[25] Kang, R., Brown, S., Dabbish, L., and Kiesler, S. B. Privacy attitudes of mechanical turk workers and the us public. In *Thenth Symposium on Usable Privacy and Security* (2014).

[26] Koshy, V., Park, J. S. S., Cheng, T.-C., and Karahalios, K. "we just use what they give us": Understanding passenger user perspectives in smart homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021).

[27] Lau, J., Zimmerman, B. J., and Schaub., F. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. In *CSCW* (2018).

[28] Lee, H., and Kobsa, A. Understanding user privacy in internet of things environments. In *Proceedings of IEEE World Forum on Internet of Things (WF-IoT)* (2016).

[29] Lee, H., and Kobsa, A. Privacy preference modeling and prediction in a simulated campuswide iot environment. In *IEEE International Conference on Pervasive Computing and Communications (PerCom)* (2017).

[30] Litman-Navarro, K. We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[31] Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., and Wagner, D. Privacy attitudes of smart speaker users. In *Proceedings of Privacy Enhancing Technologies* (2019).

[32] Mare, S., Roesner, F., and Kohno, T. Smart devices in

airbnbs: Considering privacy and security for both guests and hosts. In *Proceedings of Privacy Enhancing Technologies* (2020).

[33] Marky, K., Prange, S., Krell, F., Mühlhäuser, M., and Alt, F. "you just can't know about everything": Privacy perceptions of smart home visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia* (2020).

[34] Marky, K., Voit, A., Stöver, A., Kunze, K., Schröder, S., and Mühlhäuser, M. "i don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In *NordiCHI '20: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (2020).

[35] Martin, C. Smart home technology hits 69% penetration in u.s. https://www.mediapost.com/publications/article/341320/smart-home-technology-hits-69-penetration-in-us.html#:~:text=The%20majority%20(69%25)%20of,Consumer%20Technology%20Association%20(CTA).

[36] Montanari, A., Mashhadi, A., Mathur, A., and Kawsar, F. Understanding the privacy design space for personal connected objects. In *Proceedings of the 30th International BCS Human Computer Interaction Conference (HCI)* (2016).

[37] Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J., and Preneel, B. Collateral damage of facebook third-party applications: a comprehensive study. In *Computers & Security* (2018).

[38] Tabassum, M., Kosinski, T., and Lipford, H. R. "i don't own the data": End user perceptions of smart home device data practices and risks. In *Proceedings on SOUPS* (2019).

[39] Tabassum, M., Kropczynski, J., Wisniewski, P., and Lipford, H. R. Smart home beyond the home: A case for community-based access control. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020).

[40] Ur, B., Jung, J., and Schechter, S. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2014).

[41] Van Alsenoy, B. *Regulating Data Protection : the Allocation of Responsibility and Risk among Actors Involved in Personal Data Processing*. 2016.

[42] Williams, M., Nurse, J. R. C., and Creese, S. The perfect storm: The privacy paradox and the internet-of-things. In *2016 11th International Conference on Availability, Reliability and Security (ARES)* (2016).

[43] Yao, Y., Basedo, J. R., McDonough, O. R., and Wang, Y. Privacy perceptions and designs of bystanders in smart homes. In *Proceedings of the ACM on Human-Computer Interaction* (2019).

[44] Zeng, E., Mare, S., and Roesner, F. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security* (2017).

[45] Zeng, E., and Roesner, F. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In *28th USENIX Security Symposium (USENIX Security 19)* (2019).

[46] ZHENG, S., APTHORPE, N., CHETTY, M., and FEAMSTER, N. User perceptions of smart home iot privacy. In *Proceedings of the ACM on Human-Computer Interaction* (2018).

[47] Zheng, S., Apthorpe, N., Chetty, M., and Feamster, N. User perceptions of smart home iot privacy. In *Proceedings of the ACM on Human-Computer Interaction* (2018).

[48] Amazon Mechanical Turk. https://www.mturk.com/.

[49] Ring. https://ring.com/privacy-notice.

[50] Children's Online Privacy Protection Rule, 1998. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

[51] The General Data Protection Regulation, 2018. https://eugdpr.org/.

# A Owners' Survey

The close-ended questions in this survey are all single-answer questions.

Q1-1 Do you agree or disagree with this statement "visitors have no privacy rights in my smart home"? [Strongly disagree, Disagree, Neutral, Agree, Strongly agree]

Q1-2 Explain your previous answer:

Q1-3 When other people visit your home, do you tell them that you have smart home devices? [Yes, No, Other:]

Q1-4 When other people visit your home, do you explain what types of data are being collected about them? [Yes, No, Other:]

Q1-5 Why would you explain that to your visitors? or why not?

Q1-6 How much do you understand your smart home data practices? [Fully, Partially, Not at all]

Q1-7 How did you or how would you find information about the data practices of your smart home?

Q1-8 What would help you better understand the data practices of your own smart home?

Q1-9 Can you fully control your smart home devices like changing the settings, granting or revoking access, and controlling the collected data? [Yes, No, Other:]

Q1-10 Have you ever used any controlling features to delete collected data from any smart home device? (e.g. deleting log events, deleting audio recordings in Amazon Alexa, or others) [Yes, No, Other:]

Q1-11 What kinds of control do you have or have you used over the collected data about your smart home? What could be helpful for you to easily notify visitors about your smart home data collection, storage, and processing? [Deleting some data about me or others, Modifying some data about me or others, Sharing some data about me or others, Other:]

Q1-12 Do you know of any laws or regulations that require you to disclose the data practices of your smart home to visitors?

Q1-13 If there were specific laws or regulations that required owners of smart homes to disclose if their devices collect other people's data, would you be able to concisely write your disclosure statement? [Yes, No, Other:]

Q1-14 How would you get help writing your own smart home disclosure statement if you needed help?
Q1-15 Are there certain types of data that you collect that you would not stop collecting even if a visitor was uncomfortable? [Yes, No, Other:]
Q1-16 If a visitor (e.g., a friend, or a plumber) shows discomfort about some data practices, what would you do to address their discomfort?
Q1-17 If your family member shows discomfort about some data practices of your smart home, would you address their concern? [Yes, No, Other:]
Q1-18 If a domestic worker (e.g., a plumber or any maintenance person) shows discomfort about some data practices of your smart home, would you address their concern? [Yes, No, Other:]
Q1-19 Please explain your answers to the previous two questions:
Q1-20 Do you use any automation websites or devices (e.g. IFTTT, Samsung SmartThings hub, Apple Home, Alexa, or others)? [Yes, No]

# B Bystanders' Survey

The close-ended questions in this survey are all single-answer questions.
Q2-1 How do you feel if you know certain devices are collecting data about you while you're visiting other people's smart home?
Q2-2 Do you expect owners of smart homes to tell you about the data practices of their smart homes? [Yes, No, Other:]
Q2-3 Why do you expect them to tell you? or why not?
Q2-4 What types of data do you think are sensitive?
Q2-5 What types of data practices would you like to be notified about if you are in other people's smart home? [I would like to know what data about me will be collected, I would like to know where data about me will be stored, I would like to know how data about me will be shared, Other:]
Q2-6 How would you like to be notified about the data practices if you are in other people's smart homes?
Q2-7 Please explain your answer to the previous question:
Q2-8 What would you do if the owner of the smart home does not respect your privacy preferences? [I would not enter their smart home, It is their home so I have no say, I would not mind if my pictures and audio are recorded, I would appreciate it if my pictures and audio are not recorded, Other:]
Q2-9 If an owner of a smart home and a visitor have some conflicts regarding what data should be collected, what do you think is the best way to resolve it? [The visitor has no rights and the owner is the only decision maker, There should be some negotiation about it, Other:]
Q2-10 Some owners of smart homes might have better technical backgrounds than others. Would that influence your decision on whether you share your data in their smart homes? [Yes, No, Other:]
Q2-11 Explain your answer to the previous question:
Q2-12 What would make you share data with owners?

# C Negotiable Data Practices

We presented the same questions and answer options for both owners and bystanders. The close-ended questions in this set are all multiple-answer questions.
Q3-1 What are you willing to negotiate with visitors about collecting data about them? [Turning off all smart home devices, Turning off all smart home devices only in some rooms, Changing the frequency of the collection (collecting indoor snippets every 5 minutes instead of every second), Hiding some data (blurring the faces in indoor footage, adding noises to audios, or others), Stopping the collection of some types of data (e.g., videos), No negotiation!]
Q3-2 What are you willing to negotiate with owners about the collection of your data?[Turning off all smart home devices, Turning off all smart home devices only in some rooms, Changing the frequency of the collection (collecting indoor snippets every 5 minutes instead of every second), Hiding some data (blurring the faces in indoor footage, adding noises to audios, or others), Stopping the collection of some types of data (e.g., videos), No negotiation!]
Q3-3 Please explain your answer to the previous question:
Q3-4 What are you willing to negotiate with visitors about storing data about them? [Storing data temporarily (e.g. all data will be deleted after 3 days), Only storing data locally (not in the Internet), Storing data in a third party cloud where both (visitors and you) have equal access (e.g. both can delete collected data), Hiding some data (blurring the faces in indoor footage, adding noises to audios, or others), No negotiation!]
Q3-5 What are you willing to negotiate with owners about how your data is stored? [Storing data temporarily (e.g. all data will be deleted after 3 days), Only storing data locally (not in the Internet), Storing data in a third party cloud where both (visitors and you) have equal access (e.g. both can delete collected data), Hiding some data (blurring the faces in indoor footage, adding noises to audios, or others), No negotiation!]
Q3-6 Please explain your answer to the previous question:
Q3-7 What are you willing to negotiate with visitors about sharing data about them with others? [No sharing, Sharing but will let visitors know about the sharing, Sharing and will compensate visitors for their data, Sharing after receiving approvals from visitors, No negotiation!]
Q3-8 What are you willing to negotiate with owners about sharing your data with others? [No sharing, Sharing but will let visitors know about the sharing, Sharing and will compensate visitors for their data, Sharing after receiving approvals from visitors, No negotiation!]
Q3-9 Please explain your answer to the previous question:

# D Screening and Demographic Questions

The close-ended questions in this set are all single-answer questions except for Q4-11.

Q4-1 What is your age group? [18-25, 26-40, 41-60, over 60]
Q4-2 What is your gender? [Male, Female, prefer not to answer, others with text input]
Q4-3 What is your occupation? [Open response]
Q4-4 What is your highest level of education? [ High school diploma, Bachelor's degree, Graduate degree (e.g. master's, or Ph.D. degrees)]
Q4-5 What was your major in school? [Open response]
Q4-6 How tech-savvy are you? [Very tech-savvy, moderate, not tech-savvy]
Q4-7 Do you have any smart home devices in your home (e.g., Amazon Alexa, Google Home, or any other internet-connected appliances)? Subtitle: "Smart home devices are Internet of Things (IoT) devices that people use in their homes. Some of the uses of smart home devices are for entertainment (e.g., smart TVs, smart speakers or gaming consoles), automation (e.g., smart sprinklers or smart thermostats), or for safety (e.g., smart indoor cameras or smart locks). A smart home is any residence that has Internet-connected devices such smart cameras, smart speakers, or Internet-connected appliances. Popular smart devices include but not limited to are Amazon Echo, Nest cameras, Ring doorbell or others)"
Answer options:[Yes, No]
Q4-8 (This is just for owners) When did you acquire your first smart home device? [Within the last three month, Within the last year, More than a year ago]
Q4-9 (This is just for owners) How many smart home devices (e.g. Amazon Alexa, Google Home, Nest thermostat...etc.) do you have in your home? [1-3, 4-10, More than 10 devices]
Q4-10 (This is just for bystanders) Have you visited a smart home before (e.g., a friend or family member's smart home)? [Yes, No, Maybe, I do not know]
Q4-11 What are the benefits of living in a smart home from your opinion? [Safety, entertainment, convenience, efficiency, others]

# E Codebook

The codebook we developed for our qualitative analysis. The themes and codes were derived from the responses to our open-ended questions.

## Owners

1. Perspectives on privacy rights of bystanders
   (a) Data types disclosures to bystanders
      i. Yes [If requested only (26%), right thing to do (47%), to avoid legal consequences (20%)]
      ii. No [Not necessary (25%), awkward (16%), to avoid making bystanders uncomfortable (24%), owners do not understand their own data practices (33%)]
      iii. What would help owners disclose [Better understanding of their own data practices, tools provided by vendors to help such as privacy policies for bystanders that owners just refer bystanders to, voice announcement by the smart speaker to notify bystanders (Activated by voice command or a sensor), special sensors to trigger the existence of bystanders, signs/pamphlet next to the devices or in front of the house]
   (b) Changes of data practices when bystanders exist an show discomfort
      i. Yes [To make bystanders comfortable, Respect]
      ii. No [Preserving device utility (Safety/Automation/etc...), Might compromise owners' privacy, Bystanders are only there temporarily, My house, my rules]
   (c) Privacy rights for bystanders
      i. Yes [To make bystanders comfortable (42%), Some privacy rights, but not equal to owners (21%), Respect (37%)]
      ii. No [Preserving device utility (Safety/Automation/etc...) (38%), Might compromise owners' privacy (29%), Bystanders are only there temporarily (10%), My house, my rules (22%)]
2. Full understanding of their own smart home data practices
   (a) Yes [Easy to comprehend (22%), Similar to my job (39%), I have friends who help me (33%)]
   (b) No [Lengthy policies (40%), Technical language(10%), Legal language (32%), Lack of incentives for vendors (6%), Hopelessness (8%), Acceptance (5%)]
   (c) What would increase understanding [Family or friends' consultation (50%), Third party analysis to avoid sugar coating (18%), Videos and info graphic (12%), Personalized policies (8%), Responsive customer Services (11%)]
   (d) Use of controlling features
      i. Yes [Easy to use (63%), Need to learn how (22%)]
      ii. No [Difficult to use (15%), No helpful materials (32%), companies make it hard to collect more data (14%)]
3. Willingness to address bystanders' privacy concerns
   (a) Willing (73% of owners)
      i. For trusted bystanders such as family and friends [To maintain a social relationship (80%), To avoid legal consequences (8%)]
      ii. For untrusted bystanders such as domestic workers [The right thing to do (44%), to avoid legal consequences (22%)]
   (b) Unwilling (27% of owners)
      i. For trusted bystanders such as family and friends [To protect the smart home utility such as home safety (42%), My house, my rules (56%)]
      ii. For untrusted bystanders such as domestic workers [To protect the smart home utility such as home safety (40%), They don't trust bystanders (26%), My house, my rules (17%)]

## Bystanders

1. Concerns in other people's smart homes
   (a) Uncomfortable (72% of bystanders) [Violation of their privacy (40%), Vulnerable if some types of data is collected about them (24%)]
   (b) Indifferent (27% of bystanders) [Hopelessness (Everything collects data) (32%), Not my house (40%), Fair trade-off for the functionalities of smart homes (28%)]

**Table (2)** The smart home devices that we used for our analysis in Section 5.1. We conducted the analysis in March 2021. Samsung, Triby, and Withings have updated their privacy policies since our analysis. They still do not mention anything about the privacy of bystanders. Physical control interface shows that bystanders could change the settings of the smart home devices without access to the corresponding mobile apps. Potential privacy-preserving features show some features that owners could use to protect the privacy of bystanders.

| Manufacturer | Model | Privacy Policy Updated Since Analysis | Mentions Bystander' Privacy | Shares Data with Third Parties | Physical Control Interface | Potential Privacy-preserving Features |
|---|---|---|---|---|---|---|
| Amazon | Echo | No | Yes | Yes | Yes | Alexa Skills/Voice Commands |
| August | Smart Lock Pro | No | No | Yes | Yes | No |
| Belkin | Wemo Smart Switch | No | No | Yes | No | No |
| Google | Dropcam | No | No | Yes | No | No |
| Foscam R4 | R4 | No | No | Yes | No | Personal Data Deletion through Email Request |
| Google | Chromecast | No | No | Yes | No | No |
| Lefun | Camera (baby monitor) | No | No | Yes | No | No |
| Nest | Thermostat | No | No | Yes | Yes | Can delete data through Nest App |
| Netmato | Weather Station | No | No | Yes | No | No |
| Omron | 7 Series | No | No | Yes | No | Collected data can be deleted for GDPR protections only |
| Ring | Doorbell | No | Yes | Yes | No | Privacy Zones - Areas where the camera is blocked from recording |
| Samsung | SmartThings Hub | Yes | No | Yes | No | No |
| Samsung | SmartThings Motion Sensor | Yes | No | Yes | No | No |
| Invoxia | Triby Speaker | No | No | Yes | Yes | Can connect to Alexa and use Amazon's privacy features |
| VOCOlinc | PM2 Smart Power Strip | No | No | Yes | No | No |
| Wemo | Smart Plug | No | No | Yes | No | No |
| Withing | Sleep Monitor | Yes | No | Yes | No | Collected data can be deleted for GDPR protections only |

2. Expectations about data disclosures by owners
   (a) Expect (38% of bystanders) [Right thing to do (37%), Respectful to do (40%), Bystanders would do it for others (20%)]
   (b) Do not expect (62% of bystanders) [Owners would not know their own data practices (72%), Not normal or awkward (10%), Not necessary to do (3%), owners are careless (15%)]
3. Notification preferences
   (a) By devices (20% of bystanders) [Verbally, Signs]
   (b) By owners via a digital means (80% of bystanders) [Email, Text, Notification on my phone via an app]
4. Data sensitivity
   (a) Video footage and pictures (90% of bystanders)
   (b) Audio recordings (65% of bystanders)
   (c) Health data (32% of bystanders)
5. Willingness to share data with owners
   (a) What bystanders would do if owners do not honor their privacy preferences [not enter the home (40%), Hopeless because it is not my home, try to find middle ground (43%), Acceptance (24%)]
   (b) What should happen if they had privacy disagreement between owners [there should be some negotiation (68%), I have no rights in other people smart homes (18%), I need more explanation from owners (10%)]
   (c) Willingness to share with owners [If they consented and they trusted owners (65%), If they trusted vendor (10%), If they have some assurance about data protection (15%)]

# F List of 17 Devices

Table 2 shows all the devices we analyzed in Section 5.1.