Exploring Tenants' Preferences of Privacy Negotiation in Airbnb

Zixin Wang, *Zhejiang University;* Danny Yuxing Huang, *New York University;*
Yaxing Yao, *University of Maryland, Baltimore County*

https://www.usenix.org/conference/usenixsecurity23/presentation/wang-zixin

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the
32nd USENIX Security Symposium
is sponsored by USENIX.

Exploring Tenants' Preferences of Privacy Negotiation in Airbnb

Zixin Wang[1], *Danny Yuxing Huang*[2], *Yaxing Yao*[3]
[1]*Zhejiang University,* [2]*New York University,* [3]*University of Maryland, Baltimore County*

Abstract

Literature suggests unmatched or conflicting privacy needs between users and bystanders in smart homes due to their different privacy concerns and priorities. A promising approach to mitigate such conflicts is through negotiation. Yet, it is unclear whether bystanders have privacy negotiation needs and, if so, what factors may influence their negotiation intention and how to better support the negotiation to achieve their privacy goals. In this paper, we investigate these questions in the context of Airbnb, a special case where tenants can be considered bystanders. We conducted a vignette study that varied across three categorical factors, including smart home device types, device location, and duration of stay, with 867 participants in the context of Airbnb. We further examined our participants' preferences regarding with whom, when, how, and why they would like to negotiate their privacy. Our findings showed that device type remained the only factor that significantly influenced our participants' negotiation intention. Additionally, we found our participants' other preferences, such as contacting Airbnb hosts first to convey their privacy needs through asynchronous channels (e.g., messages and emails). We summarized design implications to fulfill tenants' privacy negotiation needs.

1 Introduction

In recent years, Internet of Things (IoT) devices are becoming ubiquitous in home environments, converting them into smart homes. These devices have enabled numerous advanced features that make people's lives easier. For example, users can remotely control, access, and monitor their smart homes to ensure home safety [14, 32]. At the same time, however, the massive data collection capability of smart home devices also raises significant privacy concerns among users, such as continuous data collection [64, 68], unspecified data sharing [9, 30, 36], and opaque data processing [8, 60]. These privacy issues also involve people other than the users, i.e., bystanders. In this paper, we use bystanders to denote people who are neither the owners nor the primary users of smart home devices but are subject to data collection, such as guests and visitors [6, 40, 41, 61], and nannies [11, 12].

One important privacy issue around smart home devices relates to the tension between smart home users and bystanders, which is generally caused by different or conflicting needs, imbalanced power dynamics, social relationships, etc [38, 51, 61, 65]. A promising direction to mitigate such tension is through negotiation. The idea of negotiating privacy preferences and options is not new. For example, in the context of drones, Yao et al. proposed a "controller-bystander app" so that drone bystanders can communicate their privacy preferences and expectations with the controller [62]. The goal of such negotiation is to communicate and settle potential conflicts between users and bystanders. Yet, it is unclear how to support such negotiation, especially in smart homes.

In this research, we take one step back from the literature – instead of proposing designs or solutions for privacy negotiation, we are interested in whether bystanders need privacy negotiation and, if so, what their negotiation preferences are in terms of when to negotiate, with whom to negotiate, and the goals of such negotiation. Studying these questions helps us gain a more fundamental understanding of how bystanders, who are in a less advantageous position to control and protect their privacy, may collaboratively address their privacy needs in an emerging technological context. As such, our overarching research question is, *how to support privacy negotiation between users and bystanders in smart homes?*

To attempt to study this broad research question, we rescope the problem and focus on a smart home environment in this paper, i.e., Airbnb rental properties. In particular, Airbnb context involves a specific type of bystanders, i.e., tenants. Tenants in Airbnb are bystanders because they are neither the owners nor primary users of smart home devices, yet their data may be collected during their stay in the rental property. We focus on the Airbnb context for three reasons. First, many Airbnb hosts have opted to install smart home devices in their rentals for different purposes [22, 26], turning the rentals into temporary smart homes. Tenants' data may be collected dur-

ing their stay, yet as bystanders, they do not have equal access to the devices nor the data collected by the devices as the hosts do. As such, their privacy may potentially be invaded. Second, while prior research has demonstrated tenants' various privacy concerns when staying at Airbnb rentals [22, 39], there is a lack of effective means for communicating their privacy needs. Finally, Airbnb is a natural environment for different types of conflicts between hosts and tenants, such as hosts' willingness for home security and tenants' need for privacy [16, 39], hosts' incentive to pursue tenants' satisfaction and tenants' expectation of their privacy to be respected, etc. These tensions and conflicting needs between hosts and tenants make Airbnb a perfect context to study privacy negotiation as a potential solution. Furthermore, in this study, we focus on the tenants' perspective, aiming to explore whether and how Airbnb tenants expect to negotiate their privacy with the hosts. We ask the following two research questions:

- **RQ1:** Do tenants have the need to negotiate their privacy with the hosts, and if so, what are the factors that influence tenants' privacy negotiation intention in Airbnb?
- **RQ2:** What are tenants' privacy negotiation preferences in Airbnb?

We conducted a full factorial vignette study with 867 participants to investigate whether and how Airbnb tenants negotiate their privacy with the hosts when surrounded by different types of smart home devices. In particular, we examined how the following three factors influence tenants' intention to negotiate their privacy needs: 1) device type, 2) device location, and 3) tenant's duration of stay in Airbnb. Our results suggest that *device type* remains the only factor that significantly impacts participants' comfort level in an Airbnb with smart devices and their privacy negotiation intention. Furthermore, participants considered the Airbnb host as their first contact point for privacy negotiation, and they preferred to use indirect ways for negotiation, e.g., sending messages and emails, rather than making direct calls.

This paper makes the following contributions. First, to the best of our knowledge, this is the first study to systematically investigate tenants' needs for privacy negotiation in Airbnb and their preferences for undertaking such negotiation. The results shed light on efforts that empower bystanders to take control of their privacy in smart environments. Second, we draw design implications on supporting privacy negotiations among Airbnb hosts and tenants.

2 Related Work

In this section, we review prior literature on different stakeholders' privacy concerns in smart homes and privacy conflicts. We then summarize prior research on mitigating the mismatched privacy preferences and the factors impacting it.

2.1 Privacy Conflicts Among Different Stakeholders in Smart Homes

Smart home privacy issues have been studied extensively. Users' common privacy concerns include transparency of data collection, data sharing, and private data security [33, 46, 59, 60, 64, 68]. Smart homes often also involve other stakeholders, such as bystanders, and different stakeholders have their own perspectives about smart home devices. Thus, privacy conflicts frequently happen among various stakeholders in smart homes [61]. Regarding surveillance, parents want to check the effects of parenting technology by watching and listening to their children's data [5, 45, 49, 56]. But children were concerned about excessive monitoring and control by their parents [45, 56]. The concerns about surveillance also appeared in nannies, home care attendants, house cleaners, and maintenance workers [11–13]. For example, nannies agreed that homeowners might install smart cameras to ensure their children's safety, but they still needed more transparency to avoid possible privacy invasion [12]. Regarding data sharing, Airbnb guests used Smart TV for entertainment but were unwilling to share their usage data, even though some hosts might want to access that data [39]. Last but not least, users' and bystanders' unequal access to smart home devices may cause privacy violations [27, 54, 64], i.e., the owner of smart homes generally has more access to functionality and data than other users [27]. Even though researchers have been trying to promote equal access in a multi-stakeholders context [29, 31, 65], the widespread application of design changes in smart devices still needs more time to adapt.

On a different node, Cobb et al. studied 386 incidental users of smart devices. While participants were interested in technical implementation to solve their privacy problems, they frequently expected an open dialogue with device owners to negotiate privacy needs [19]. That particular direction points to a promising way to mitigate the conflicts and tension among multiple stakeholders, i.e., through negotiation.

2.2 Why Privacy Negotiation?

Extensive research found multiple ways to mitigate conflicts between different stakeholders. Prior studies have created multi-user systems to mitigate the conflicts between different stakeholders [51, 65]. Other users also tend to cooperate and even negotiate with owners about their privacy concerns [61, 62].

Negotiation is considered a reactive protective behavior in interpersonal privacy management [17, 21]. Compared with other privacy protection behaviors, which mostly support single-user preferences, negotiation can help more than one user and bystander. Sikder et al. designed a policy negotiation mechanism to resolve conflicting demands and found more than half of the participants suggested that the users and members should be notified to negotiate together when they were

in privacy conflicts [51]. Prior work has documented negotiations between parents and children in a smart home [27]. These findings indicated that there was a negotiation means to mitigate bystanders' concerns. However, details, such as how they can negotiate and what goals they want to achieve after negotiation, were still largely missing. We aim to fill this gap by systematically examining whether individuals, especially bystanders, have the need to negotiate and how they solve their privacy concerns via negotiation.

2.3 Factors Impacting Intention to Negotiate

Studies on negotiation-based privacy-protective behaviors (PPBs) have identified different factors influencing people's intention to negotiate. We summarized three main perspectives: gender, social factors, and perceived vulnerability.

Gender. Wilkowska and Ziele's study showed that female adults had more stringent security and privacy standards than male adults about using e-health technologies at home [58]. De Wolf [21] investigated the predictors of teens' interpersonal PPBs on social media. The results show that Belgian females were more cautious than men in protecting privacy, such as negotiating what can be posted with friends. In contrast, McGill and Thompson found that the security behaviors of male users were stronger than female users' [44]. Chou et al. [17] regard PPBs with interpersonal dynamics as reactive PPBs and found that male students were more inclined to take reactive privacy protection, such as negotiation, than female students. Thus, the influence of gender on negotiation behaviors is still inconclusive.

Social factors. Users' relationship is a main factor to drive human disclosure of personal information on social media [57]. Such et al. [53] designed an automatic negotiation mechanism based on the social relationship between users, and proved that social relationship was the determining factor that affects users' PPBs. Chen et al. [15] found that social distance was a significant predictor of perceptions about Internet privacy risks. Besides, some people prioritized maintaining social norms or avoiding the potential social confrontation, so they were less inclined to take action even though they still cared about their own privacy [11, 55, 66].

Perceived vulnerability. Perceived vulnerability refers to the judgment of a person's sensitivity to privacy invasion in the IoT world. Youn et al. [63] found that perceived vulnerability significantly correlated with proactive PPBs. Compared with proactive PPBs, with a higher level of perceived vulnerability, people were more likely to choose creative PPBs [17]. A meta-analysis of studies on Protection Motivation Theory and information security behavior showed that response costs (i.e., in terms of effort or time for protection) reduce one's willingness to engage in risk-reducing behavior [52].

Our research builds on this prior work and explores the factors that may influence tenants' privacy negotiation intention and preferences in Airbnb and how to support privacy negotiation in future smart homes broadly.

3 Methodology

To answer our research questions, we conducted a vignette study with 867 participants after screening the low-quality ones. We present the details below. The study is approved by our institution's IRB.

3.1 Participants Recruitment and Eligibility

We implemented our survey using Qualtrics and recruited our participants through Prolific. We framed our research as "a project to understand your smart home experiences." To avoid the impact of previous TikTok incidents on Prolific sample [28] , we selected the "gender balanced" sample for our recruitment. We then distributed the survey over one week in batches of 100. We deliberately released each batch at different times of the day on different days of the week to account for participants who work on different schedules. We also selected the "even distribution" option on Qualtrics to ensure an even distribution of all vignettes.

On Prolific, we set the recruitment criteria to filter participants who are at least 18 years old, located in the US, fluent in English, and have over 95% task approval rate. All respondents first participate in a screening survey - as we focus on Airbnb tenants, we use the screening survey to filter eligible respondents with prior Airbnb experience. All participants would sign the consent form through Qualtrics before seeing the screening survey. We did not ask about participants' experiences with smart home devices, as anyone can be a tenant in Airbnb and encounter smart home devices during their stay, regardless of their prior experience. The average completion time of the screening survey was 0.89 minutes, and participants received $0.2 after completing the screening survey (equaling $13.4/hr, higher than our local minimum wage $13.25/hr).

After finishing the screening survey, all eligible participants continued to take the full survey after signing another consent form. Upon participants' completion, we removed 32 low-quality responses, including fast responses (i.e., <1min for the main survey), duplicated entries (i.e., exact same responses from two different Prolific IDs), and clear copy-and-paste (i.e., same text for all open-ended questions). The average completion time of the full survey was 7.9 minutes. Those who finished the full survey would receive another $1.8 bonus, making the total compensation $2 (equaling $13.65/hr, higher than our local minimum wage $13.25/hr).

3.2 Research Ethics

Throughout the research, we took extra care of our research ethics and implemented the following strategies to ensure an ethical research approach in all aspects. First, all participants

Factor	Levels	Description
Device type [46]	Door/Window Sensor; Gaming Console (e.g., Xbox, PlayStation); Motion Sensor; Smart Appliance (e.g., smart light, power outlet,); Smart Camera (e.g., Nest camera); Smart Thermostat (e.g., Nest thermostat); Smart TV (e.g., TV with Wi-Fi); Voice Assistant (e.g., Amazon Echo)	The device that collects data
Device location [3, 39]	Public area; Shared room; Private room	The location where the smart home device is installed
Duration of stay [61]	One day; Three days; One week	The duration that tenants will stay

Table 1: Factors varied between vignette scenarios, levels of the factors presented in scenarios, and description of each factor.

were required to consent forms for both the screening survey and the main survey. Due to the two-layer payment structure in our study, we clarified the compensation in both consent forms to reduce any possible confusion. Second, we did not collect any personally identifiable information in the study. The only identifier for our participants is their unique IDs from Prolific, which consist of random numbers and letters. Third, when we rejected low-quality responses, we provided a short explanation to the participants.

3.3 Pilot study

Before running the formal study, we launched three batches of pilot studies to test our screening mechanism, survey flow, and survey logic. We identified any potential errors in displaying the vignettes. In total, we collected sample data from 31 participants.

We further used the pilot data to do a power analysis. With an 80% power (power = 0.8), medium effect (f2 = .25), and a significance level $\alpha = .05$, the minimum required sample size was N = 636 for the general linear model.

3.4 Survey Design

In this section, we introduce the structure of our survey. The complete survey protocol can be found in the Appendix.

Our main survey contains four main parts. In the first part, we start by asking participants about their experiences with smart home devices, such as the types of devices they own and how long they have been using their devices. We then ask about participants' overall comfort level with smart home data collection.

The second part involves a vignette study regarding a data collection scenario in Airbnb. To construct the vignettes, we reviewed the literature and identified a set of factors, including "data purposes", "data retention", "data access", "data type", "device types", "device locations", and "duration of stay". After reviewing all factors carefully, we removed the first three factors because 1) information such as "data retention" and "data access" is generally not available to tenants when they arrive at an Airbnb, yet they have to make their negotiation decisions without that information; 2) "data type" and "data purposes" are highly relevant to individual SHD. Including them invalidates many vignettes (e.g., voice assistants collect food preferences to order food), similar to Emani-Naeni et al.'s approach [46].

Eventually, we deliberately selected three factors that may influence people's negotiation intention , i.e., device type, device location, and duration of stay. Each factor further has several levels, which were informed by either prior work [39, 46, 61] or the settings on Airbnb [3]. The details of the factors and their levels are presented in Table 1.

Based on our selection of factors, we iteratively created the following template for our vignette:

Imagine the following scenario: you are staying in an Airbnb alone for ***three days*** *and the* ***Smart Camera (e.g., Nest camera)*** *present in the* ***shared room*** *is collecting your data.*

For each vignette, we first ask participants how comfortable they were with the data collection in this scenario. Then, through several multiple choice questions, we ask participants what privacy protection strategies they would like to use in this scenario, whether they would like to negotiate their privacy options, and if so, how/when/why with whom will they negotiate. To ensure that all participants have a similar understanding of the concept of negotiation, we used "communicate and discuss (i.e., negotiate)" for clarification (e.g., ***Who*** *would be your preference to* ***communicate and discuss (i.e., negotiate)*** *your privacy preferences with?*)

It is worth noting that, to ground the choices for these multiple-choice questions, we adopt two strategies. First, we reviewed prior literature and adopted the choices from them. For example, take actions on your own, such as unplugging the devices [33]. Second, for some questions that do not have

support from prior literature, we first used open-ended questions to source popular options from our participants. We elicited options based on the response and used them as the choices for the multiple-choice questions in the final version.

In the third section, we asked participants how having a travel companion staying in Airbnb together would impact their negotiation intention. For each participant, the travel companion may have one of the following seven types of social relationships with them: "close relatives", "close friends", "colleagues in the same organization", "people in the same occupation", "domestic strangers", "someone you don't know". This is based on a social scale inspired by [15, 48]. We asked this question because literature has suggested that social relationship remains one factor that impacts people's privacy perceptions in smart homes [11, 27, 55]. Specifically, we asked them when they travel with different companions instead of going alone, whether their negotiation intention will increase or decrease, and why. We chose to include this factor in a separate question rather than having it in the vignette for two reasons. First, we are interested in the directions of change (increase or decrease) for each participant—thus, a separate question will allow a within-subject investigation. Second, including social distance as a factor in the vignette will significantly increase the number of vignettes and, thus, the cost of the study, so practically, we opted not to do so.

In the final part, we included demographic questions and questions regarding participants' technical level.

3.5 Data Analysis

We collected both quantitative and qualitative data through the survey. We detail our data analysis to investigate the impact of three factors (i.e., device types, device location, and duration of stay) on participants' comfort level with the smart devices in the given scenario and their intention to negotiate their privacy needs.

Quantitative data. We defined two measures, i.e., comfort level in the given scenario (4-point Likert scale) and intention to negotiate their privacy needs (4-point Likert scale). Since these two measures are ordinal, we fitted two Cumulative Link Mixed Models (CLMMs) for our analysis [18]. Via the CLMM analysis, we found a significant effect of device type on participants' comfort level ($\chi^2(7,\ N = 867) = 48.16$, $p < .000$) and intention to negotiate their privacy needs ($\chi^2(7,\ N = 867) = 28.45$, $p < .000$).

After CLMM analysis, we conducted post hoc multiple comparisons via Estimated Marginal Means to investigate the relationship between different levels of device type. We corrected the p-value with Tukey HSD Correction.

Specifically, regarding how different social relationships influence participants' intention to negotiate their privacy needs, we used Analysis of Variance. We found that the type of social relations has a significant effect on participants' intention to negotiate ($F(5, N = 867) = 3.21$, $p = .007$). We corrected the p-value with Games-Howell Correction based on unequal variances.

Qualitative data. For each open-ended question, two researchers collaboratively coded a subset (n=100) of data using open coding (i.e., inductive coding). They conducted multiple rounds of discussions to reach a full agreement and generated an initial codebook. Due to a large amount of data, a third coder was brought in to help with the coding. We trained the third researcher using the same process, i.e., all three researchers repeated the same open coding process on another subset of the data (n=100) to ensure a consistent understanding of the data and a full agreement with the coding, then updated the codebook as needed. Three researchers then split the rest of the data and coded it individually using the agreed codebook. Each response was coded by two researchers (i.e., each researcher coded two third of the data). To ensure consistency in the coding process and reduce ambiguity in the codes, all researchers discussed their codes regularly and iteratively refined the codebook as needed. Disagreements in the coding were discussed until all researchers agreed (e.g., an initial code "avoid social faux-pas" was changed to "avoid embarrassment" to reflect the participants' responses accurately). During the discussion, whenever an initial code was changed, all coders would go through the coded data and update the codes accordingly (including the ones in the training dataset). This is a similar coding process to that in the prior work [37]. Since the coding involved constant discussions and iterations and eventually reached a full agreement, the inter-coder agreement is not necessary [43]. The final codebook can be accessed through Open Science Framework [1].

3.6 Limitations

This paper has some limitations that need to be considered when interpreting the results.

First, this study focused on Airbnb, a specific context that may contain smart home devices. Airbnb offers a unique environment to study tenants as bystanders since when staying in an Airbnb rental, tenants typically do not have access to the data collected by the installed smart devices or additional information on the data practices (e.g., purposes, retention, data types, data retention, etc.). However, the Airbnb context also represents several unique characteristics that may change tenants' privacy expectations and behaviors (e.g., tenants having to pay to stay in a rental). As such, our results may not generalize to the privacy negotiation behaviors of bystanders in other smart environments.

Second, in the scope of this study, we did not consider the perspective of Airbnb hosts. We did not investigate how hosts may react to tenants' negotiation requests and perceive the appropriateness of such requests. As such, the results should be interpreted from the tenants' perspective.

[1] https://osf.io/c43j5/

Gender		Age		Education		Airbnb?		Smart devices usage	
Male	48.0%	18-24	26.2%	High school	28.5%	Past year	46.3%	< 3 mo.	17.6%
Female	49.3%	25-34	41.4%	Bachelor	51.0%	Past six months	33.7%	3 mo. - 1 yr	16.5%
Non-binary	2.7%	35-44	21.0%	Master	14.6%	Past month	15.9%	> 1 yr	65.9%
		45-54	7.0%	Doctoral	4.6%	Past week	2.9%		
		55+	4.2%	Prefer no answer	1.3%	Past three days	1.3%		

Table 2: Participants' demographic information.

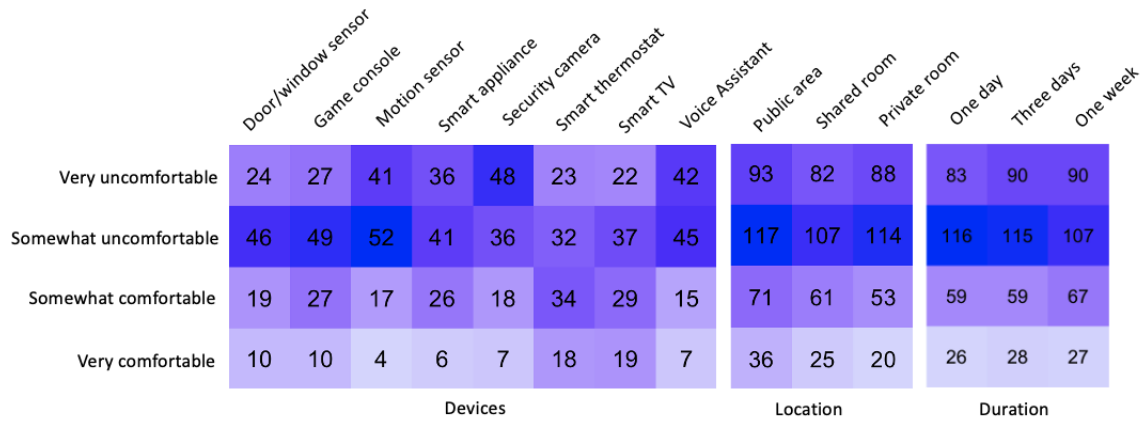

Figure 1: Summary statistics showing the relation between the factors and participants' comfort level. Each numerical value denotes the number of participants. For example, 52 participants were somewhat uncomfortable when motion sensors were presented in Airbnb.

Third, all of our participants came from the US. We did not consider cultural or other differences (e.g., legislation) that may contribute to participants' privacy perceptions and behaviors.

4 Results

4.1 Demographic Information

We received 867 valid responses. Our participants represent diverse backgrounds in terms of their genders, ages, smart home experiences, technical level, etc. All participants have recent experiences staying in an Airbnb property. This is to ensure that, when responding to our survey, our participants could build connections with their prior experiences, further increasing our data's validity. The demographic information of our participants can be found in Table 2.

4.2 Factors Impacting Comfort Level

4.2.1 Participants' self-reported comfort levels

In each vignette, we asked participants about their comfort level in the scenario on a four-point Likert scale from "Very comfortable" to "Very uncomfortable". Our descriptive analysis (Figure 1) suggested that participants were most uncomfortable when security cameras (N=48), voice assistants (N=42), and motion sensors (N=41) were presented in Airbnb. Their comfort levels related to the location of the devices and duration of stay were fairly consistent across different factors.

4.2.2 Device type significantly influences comfort level

For each vignette, we asked participants to rate their comfort level. We fitted a CLMM model to further examine factors that impact their comfort level. The results indicated that only the *device type* have a significant effect on participants' comfort level($\chi^2(7,\ N = 867) = 48.14$, $p < .000$). This is in line with the findings from prior work [46].

We did not observe a significant effect on participants' comfort level from device location ($\chi^2(2,\ N = 867) = 2.95$, $p = .228$) and duration of stay ($\chi^2(2,\ N = 867) = 3.64$, $p = .162$). This contradicts prior work suggesting that the device location [46] and duration of stay [61] may impact people's comfort level and thus. We suspect this is due to the unique social contexts in Airbnb and tenants' role as bystanders (i.e., not the owners).

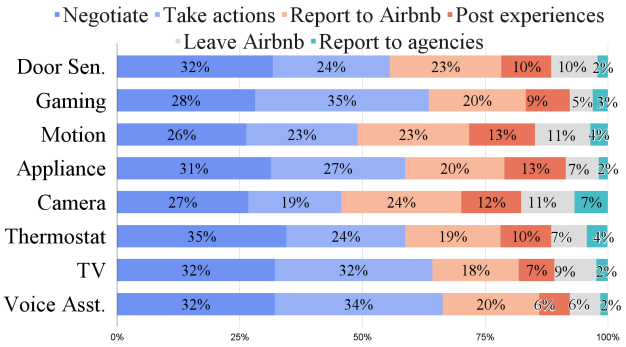

Figure 2: Participants' preferences of privacy protection actions across eight device types. Negotiation remained the most popular choice for most device types.

4.2.3 Preference on privacy protection actions

After we asked participants about their comfort level in each vignette, we continued to ask them what actions they may take when they discover the smart device usage and the data collection. Participants selected their answers from a list of choices generated from our pilot data and had the option to fill in a free response. As device type is the only factor that significantly impacts participants' comfort level, we focused our analysis on the following privacy protection actions (PPAs) based on device types: negotiate with the host; take actions on their own; report to Airbnb; post the experience publicly on social media; leave the Airbnb rental; and report to law enforcement agencies. We used the chi-square test and found a significant correlation between PPAs and device types ($\chi^2(35, N = 867) = 57.48$, $p = .009$) as well. The post hoc comparison tests with correction showed that participants were most likely to choose to negotiate their privacy when a security camera was presented in the scenario ($n = 59$, $p = .008$). Figure 2 showed that the most popular PPAs were through negotiation and taking actions on their own. The results further indicated that an open negotiation between tenants and the users was still a promising approach.

4.3 Factors that Impact Participants' Privacy Negotiation Intention

Aside from participants' overall comfort level, we are particularly interested in 1) whether our participants would like to negotiate their privacy and 2) how different factors influence their negotiation intention.

4.3.1 Participants' self-reported privacy negotiation intention.

In the survey, after presenting the vignette, we asked participants their privacy negotiation intention in the scenario on a four-point Likert scale from "Very likely" to "Very unlikely". Based on the descriptive data, Figure 3 shows the distribution of participants' negotiation intention across different levels of each factor in the vignettes. We noticed that participants were most likely to report that they would negotiate their privacy when motion sensors (N=47) and security cameras (N=46) were presented in Airbnb. Their negotiation intention related to the location of the devices and duration of stay were fairly consistent across different factors.

4.3.2 Device type has a significant impact on people's negotiation intention.

Similarly, we fitted a CLMM model to explore how device type, device location, and duration of stay influence participants' negotiation intention. A CLMM model showed that *device type* has a significant effect on participants' privacy negotiation intention in an Airbnb ($\chi^2(43, N = 867) = 25.50$, $p < .000$). We did not find a significant effect from device locations ($\chi^2(43, N = 867) = 1.08$, $p = .583$) and duration of stay ($\chi^2(43, N = 867) = 1.31$, $p = .518$). We also noticed a marginally significant effect between device type interaction ($\chi^2(43, N = 867) = 21.93$, $p = .079$) with the duration of stay and participants' negotiation intention.

Specifically, participants were more likely to negotiate their privacy needs when a room includes a motion sensor than a gaming console (*mean difference* = -0.40, $p = .027$), smart TV (*mean difference* = -.39, $p = .010$), and smart thermostat (*mean difference* = -0.45, $p = .044$). This aligns with the findings from prior work [39], which indicated that Airbnb guests were more sensitive to motion sensors than entertainment devices. Our results also suggested that participants were more likely to negotiate when their room is equipped with a camera than a smart TV (*mean difference* = -0.39, $p = .039$). The complete pairwise comparison results can be found in Open Science Framework[2].

4.3.3 Comfort level is negatively correlated with negotiation intention.

We further investigated whether there was a correlation between participants' comfort level and their negotiation intention via analysis of variance. We found that participants' comfort level has a negative correlation with their intention to negotiate ($F(43, N = 867) = 63.25$, $p = .023$). In other words, the higher participants' comfort level was, the less likely they would negotiate their privacy.

4.3.4 Reasons why/why not participants negotiate their privacy.

We asked our participants why or why not they would negotiate their privacy. We conducted a thematic analysis and

[2] https://osf.io/c43j5/

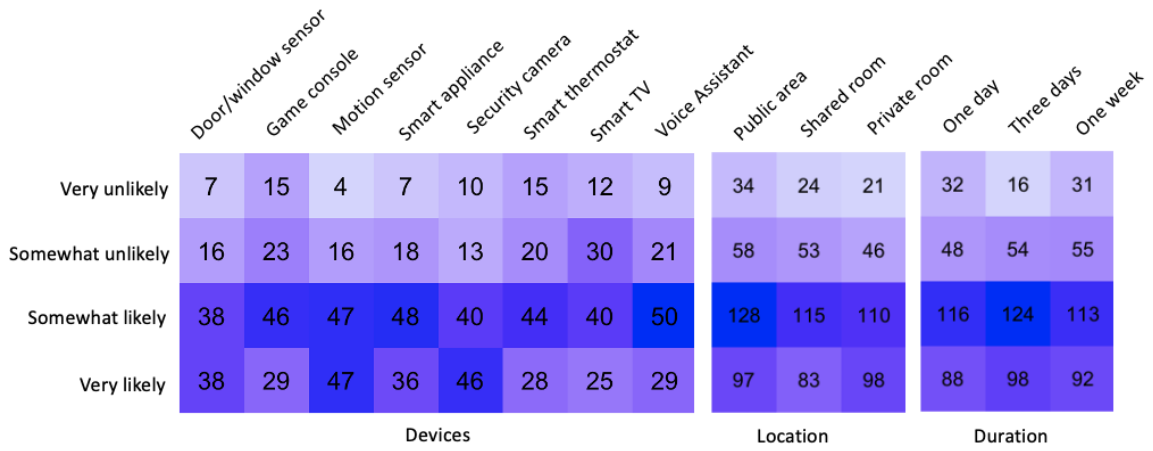

Figure 3: Summary statistics showing the relation between the factors and participants' negotiation intention. For example, 47 participants indicated that they were very likely to negotiate their privacy when motion sensors were presented in Airbnb.

summarized the main themes of participants' rationale, representing their considerations when deciding whether they would negotiate their privacy or not. For example, for those who are willing to negotiate, many of them (N=233) have certain goals in mind, e.g., seeking privacy controls and solutions. They may also negotiate because of privacy concerns (N=173), protecting their privacy rights (N=105), and interestingly, considering some potential social impact (N=132), such as to avoid social confrontation (i.e., some participants do want to negotiate their privacy needs, but at the same time they are hesitant to raise any conflict or problems). Those who were not willing to negotiate mostly believed that they did not care about the situation or their privacy enough to take action (N=102), or they would prefer to take alternative actions (N=39), such as turning off the devices by themselves. The themes are presented in Table 3.

4.4 Participants' Preference of Privacy Negotiation

In the survey, we asked our participants several questions to understand their privacy negotiation preferences, including with whom, how, when they would like to negotiate, and why. The results are presented below.

4.4.1 "Who": Airbnb hosts were the most popular choice to negotiate with.

Figure 4 shows our participants' selection of with whom they would like to negotiate. The results suggested that most of our participants believed they should negotiate their privacy options with Airbnb hosts.

Through the open-ended responses, we further identified several considerations that our participants had when deciding with whom to negotiate. The top consideration, to our surprise, is the social factors (N=81). For example, 49 participants would negotiate with the Airbnb host or Airbnb because they did not intend to escalate the case beyond Airbnb or the hosts, such as to law enforcement agencies. Other considerations include which channel is the fastest to solve their issue (N=60), the device ownership (N=39), who should take responsibility (N=31), who should ensure their user rights (N=30), whether the data collection is legal (N=21), and other (N=8).

Participants further explained some considerations they had when they tried to decide with whom they should negotiate. Interestingly, social factors remained the most considered items. For example, participants who would negotiate with Airbnb and hosts mentioned that they did not want to escalate the issue beyond Airbnb and host to entities such as law enforcement agencies and third parties. Another main reason why many participants would negotiate with hosts was that hosts, as device owners, should be able to address their concerns faster than other entities. We include the complete list of considerations and the associated codes in Table 4 in detail.

4.4.2 "How": Asynchronous communication channels were preferred for negotiation purposes.

We were also interested in the participants' most preferred way of privacy negotiation. Our data suggested that the top three most preferable negotiation channels included sending messages to Airbnb hosts (N=466), sending emails to Airbnb hosts (N=458), and sending emails to Airbnb customer services (N=361). Fewer participants chose to either call hosts (N=326), call Airbnb customer services (N=295), or talk to the host face-to-face (N=258). This is a somewhat surprising result to us since, generally speaking, synchronous communication (e.g., phone calls, face-to-face) is more effective than asynchronous communication (e.g., messages, emails) for the purpose of negotiation as a proper negotiation process would

Categories	Themes	Codes
Why negotiate? (N=643)	Achieving certain goals (N=233)	Increase transparency (N=82)
		Seek privacy controls (N=76)
		Express privacy needs (N=59)
		Make others aware (N=16)
	Have privacy concerns (N=173)	Confirm proper data practice (N=46)
		Privacy violation (N=43)
		Abnormal situation (N=30)
		Context-dependent negotiation (N=20)
		Uncomfortable (N=18)
		Surveillance (N=9)
		Data collection is unnecessary (N=7)
	Social reasons (N=132)	Inform owners of their privacy concerns (N=96)
		Avoid confrontation (N=36)
	Protecting personal rights (N=105)	Consent is needed (N=59)
		Reluctant to share private data (N=22)
		Ensure the legitimacy of data collection (N=12)
		User rights (N=12)
Why not negotiate? (N=149)	Mental peacefulness (N=102)	Don't care (N=76)
		Privacy invasion is inevitable (N=21)
		Get used to data being collected (N=5)
	Take other actions (N=39)	Turn off devices (N=33)
		Leave Airbnb (N=12)
		Change behaviors accordingly (N=2)

Table 3: A summary of reasons why or why not participants would like to negotiate.

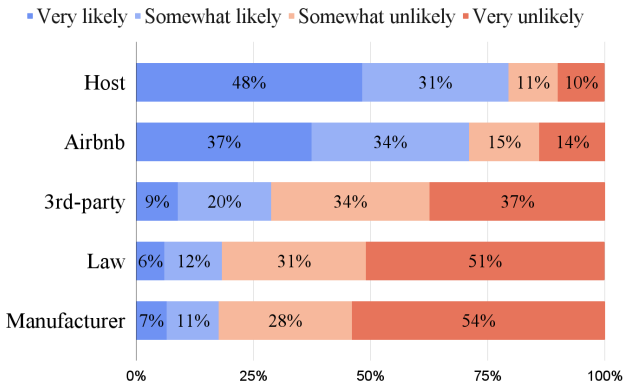

Figure 4: Whom our participants would like to negotiate with. Airbnb hosts remained the most popular choice.

involve going back and forth between the two involved stakeholders. Yet, our data suggests that our participants preferred to use asynchronous communication channels.

To further investigate this interesting phenomenon, we tested whether participants' negotiation intention impacted their preferences of how to negotiate. To do so, we converted the answers to this multiple-choice question into a list. Each participant would have a binary answer for each choice. A chi-test showed a significant effect($\chi^2(24, N = 867) = 45.20$, $p = .006$) after Bonferroni correction on the p-value. That is, those with higher negotiation intention are more likely to send messages to hosts than those who are less likely to negotiate. Furthermore, aligning with the results in prior sections, participants preferred to seek help from Airbnb hosts rather than Airbnb customer service.

4.4.3 "When": Most people preferred negotiating while booking the rental.

We asked participants when they would like to negotiate their privacy needs. 60.3% of the participants prefer to negotiate on the application while booking, 22.4% of the participants prefer to negotiate at the property during check-in, 8.9% of the participants prefer to negotiate during check-out, and 6.7% of the participants prefer not to negotiate. We further test how device type impact when to negotiate. The results showed device type had a significant effect ($\chi^2(28, N = 867) = 46.85$, $p = .014$). Participants are more likely to negotiate their privacy needs in every time period when motion sensors were present in the room than other devices ($B = 2.61$, $p = .014$). Besides, When there is a smart camera in the room, participants are more likely to negotiate their privacy needs while booking ($B = 1.34$, $p = .047$).

Considerations	Codes
Social factors (N=81)	Avoid escalating conflicts (N=49)
	Law enforcement is not helpful (N=14)
	Manufacturers don't care (N=12)
	Hesitant to directly contact host (N=6)
Efficiency in negotiation (N=60)	Host can address concerns (N=24)
	Hosts can easily handle the request (N=15)
	Anyone who can address concerns (N=12)
	Airbnb is quickest (N=9)
Device ownership (N=39)	Hosts own devices (N=39)
Who is responsible (N=31)	Host is the sole responsible person (N=13)
	Host and Airbnb are responsible (N=11)
	Airbnb has the most responsibility (N=7)
User rights (N=30)	Inform Airbnb of the host violation (N=30)
Legal rights (N=21)	Contact law enforcement (N=21)
Escalation (N=8)	Involve everyone (N=8)

Table 4: Participants' considerations when deciding with whom they would negotiate their privacy.

4.4.4 "Why": Privacy negotiation goals

One important question we are interested in is what goals participants wanted to achieve through negotiation. Our analysis identified four primary goals: 1) get more information; 2) express their privacy needs; 3) seek privacy controls; 4) inform other users.

Get more information. Many participants (N=287) indicated they would like to know more about smart device usage in Airbnb and data practices, such as what data is collected, data collection purpose, who can access the data, the necessity of data collection, and retention time.

"I'd like to know why the data is being collected and for whom. Where is it stored and what exactly is being stored." (P179)

Express privacy needs. Many participants (N=275) stated that by contacting Airbnb hosts, they would like to inform the hosts of their privacy preferences. To some participants, they would like the host to know that they have privacy concerns regarding the smart device usage, such as ensuring privacy security (N=61) and personal safety (N=32), stopping data collection (N=60), needing consent while booking or being informed to being collected data (N=49).

"Just to make sure I feel comfortable and safe and like my privacy is being respected if I'm staying at a property. So I would communicate with the host in case I'm not feeling that way and I would hope that the host could communicate in a way or take steps to alleviate any concerns I had." (P758)

To some other participants, the negotiation was more like communication with the host rather than a channel through which they could seek help. In this case, privacy negotiation provides psychological support (N=73).

"I want the Airbnb host or whoever I'm speaking with, to understand me and my feelings about the devices." (P2)

Seek privacy controls and solutions. Some participants (N=259) would like to seek privacy controls or solutions to mitigate their privacy concerns through negotiation. Some participants would like direct controls that they could understand by themselves, such as turning off devices (N=68), erasing data (N=38), removing devices during their stay (N=32), and whether they can be turned off by themselves (N=22).

"Find out if the data collection could be halted or paused while I am there" (P161)

"I would like the Airbnb host to discontinue the use of data collection from the smart devices if I said I wasn't comfortable with it. (P365)

Other participants would like to seek other solutions to ensure their privacy in the future. For example, some participants aimed to receive compensation to make up for their privacy loss (N=30), provide accommodations to different customer needs in the future (N=30), keep the Airbnb owner in check or compliance with federal or state privacy laws (N=22), let Airbnb know such data collection and ensure this would never happen again in the future (N=17).

"The person to be held accountable and repercussions to be made to prevent this from occurring again." (P355)

"I believe it's illegal to try to record data of a private space. It should be reported to law enforcement and Airbnb."(P606)

Inform other tenants. Interestingly, some participants would like to let others know of potential privacy risks with smart devices and make sure the next person that stays is informed about data collection before booking (N=33).

"I want to spread awareness so people can regain privacy and also know before they book." (P184)

Categories	Codes
Increase (N=307)	More people are involved (N=80) Peer support (N=74) Be responsible for others (N=66) Need transparency (N=68) Others have the same privacy concerns (N=10) Cautious of strangers (N=9)
No change (N=142)	Negotiate needed regardless (N=43) Consistent negotiation intention (N=31) Transparency needed regardlessly (N=27) Privacy issues still exist (N=25) Don't care (N=16)
Decrease (N=111)	Avoid embarrassment (N=24) Reduced risks due to broader data collection (n = 22) Prioritize others' privacy (N=16) No time for negotiation (N=16) Safety guarantee (N=13) Feel safer when staying with others (N=10) Rely on others to solve problems (N=10)
Maybe (N=11)	Depend on others' expectations (N=11)

Table 5: Summary of reasons why participants decided to change their intention to negotiate based on who traveled with them.

4.4.5 Who is presented in Airbnb influences participants' negotiation intention.

When responding to the vignette, our participants were asked to situate in a scenario in which they were not traveling alone. We were interested in whether their negotiation intention would change if they were to travel with a companion. We characterized seven types of social relationships based on social scale [15, 48]. These seven types of social relationships are adopted to fit our study context. To prepare our data for statistical analysis, we first coded the changes in their negotiation intention into four categories, i.e., "increase", "decrease", "maybe", "no change". The distribution of changes over the different social companions is shown in Figure 5. Then, we coded the reasons for their stated change/no change.

We noticed that when traveling with close relatives and family members, our participants' intention to negotiate their privacy is significantly higher than other types of social relationships. The open-ended responses provide further insights into why our participants' negotiation intention would increase or decrease. For those whose negotiation intention increased, they believed that once they had travel companions, more people would be at risk (N=80). They would like to provide peer support (N=74) and remain responsible for others (N=66). For those whose negotiation intention decreased, they believed that negotiating privacy while others were present may drag them into a social faux pas (N=43). In addition, some participants believed that when there were more people in the Airbnb rentals, the data collection would be about all people in the room rather than a certain individual; thus the privacy risks decreased (N=22). It may also depend on other people's privacy expectations (N=16). A complete list of themes regarding why our participants' negotiation intention changed/unchanged can be found in Table 5.

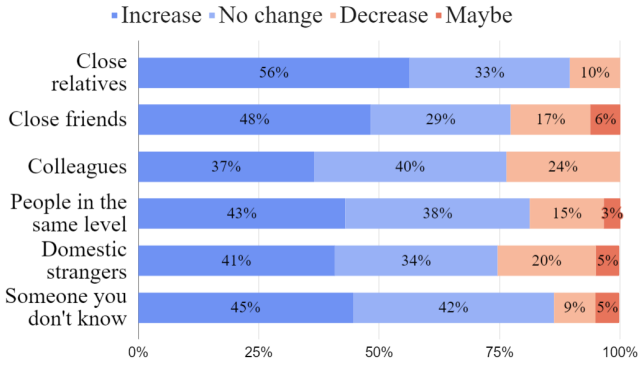

Figure 5: Negotiation intention changes with different social companion

5 Discussion

In this study, we explored Airbnb tenants' preferences of privacy negotiation when they encounter rentals in which smart home devices are installed. We found that the device type was the only factor that may influence participants' comfort level and their negotiation intention, while the location of the devices and tenants' duration of stay did not have a similar impact. Our yield insights on participants' preferences of privacy negotiation, e.g., the majority of our participants would like to negotiate with Airbnb hosts; most participants preferred to negotiate while booking the rental; and most participants preferred to negotiate through asynchronous communications channels (e.g., text messages) rather than synchronous ways (e.g., phone calls, face-to-face conversations).

Based on our results, we consider privacy negotiation a promising way to mitigate the tensions and conflicts between tenants and hosts and address tenants' privacy needs when staying at a sensorized Airbnb rental. In this section, we first discuss the tensions between Airbnb hosts and tenants as we observed in our study, and then provide a reflection on our results comparing with the prior literature and Airbnb policies. Finally, we draw implications for both Airbnb and the hosts.

5.1 Tension Between Hosts and Tenants

One fundamental rationale behind the notion of negotiation relates to the conflicting interests between hosts and tenants.

From the hosts' perspective, they typically have legitimate reasons for installing smart devices in their rental properties. For example, Airbnb hosts may install smart home devices to meet various needs of tenants (e.g., convenience, easy access, cool, etc.). They may also install smart home devices to ensure the safety and security of their property (e.g., tenants damaging the property [20, 23, 47, 50]) or their personal physical privacy (e.g., tenants invading their personal space in a shared rental). However, as prior research has suggested, tenants would be concerned about their privacy when staying in an Airbnb rental, such as data collection, data sharing, data misuse, surveillance, etc [16, 39]. Some tenants also believed that during their stay, they should have full access to the smart devices as well as the data collected by these devices. Furthermore, when discovering smart devices when staying in an Airbnb rental, many tenants in our study suggested that they would simply disconnect the devices or turn them off without informing or communicating with the hosts, making the smart devices unusable. As a result, we observed the tension *between hosts' needs for their intended utility and tenants' needs for privacy.*

Such tension also exists in Airbnb's policies. Airbnb's policy states that the hosts are responsible for installing any monitoring devices in a visible manner and disclosing them in the listing description. The policy specifically restricts the use of security cameras and other recording devices in the rental property and requires hosts to disclose the presence of these devices in the listing [2, 3]. However, Airbnb also states that tenants may not disconnect or otherwise obscure any permissible and properly disclosed security devices [4]. We believe that the current policies of Airbnb further intensify the tension between hosts and tenants and, at the same time, introduce new tension between tenants and the Airbnb platform for two reasons. First, the existing policy requires disclosure of the *device presence* rather than *the data practices of the devices*. As a result, such disclosure provides very limited information for tenants to make informed privacy decisions. Second, the current policy also puts tenants in a significantly disadvantageous position when pursuing their privacy. When they discover smart devices in their rental, tenants have very limited options: They either accept the presence of smart home devices and the fact that their privacy may be at risk, or search for a new listing. Oftentimes, tenants may be forced to choose the former option due to many practical reasons (e.g., premium location, reasonable price, etc.), but at the cost of their privacy.

Thus, we believe that enabling privacy negotiation between tenants and hosts may provide a variable solution for such tension. Clear communication of each stakeholder's needs and a set of properly negotiated strategies may fulfill the needs of both tenants and hosts. Next, we reflect on our study results with additional insights.

5.2 Reflection on Our Results

In this section, we further reflect our results in the literature, including how our results echo or contradict the findings from prior work.

Prior work has consistently suggested that device types would influence people's privacy perceptions in smart homes [10, 46, 60] . Our findings echoed the literature, then further showed that device types also significantly impact our participants' privacy negotiation intention. For example, participants were more inclined to negotiate their privacy when motion sensors were presented in a rental property compared to when other devices (e.g., smart thermostat, entertainment devices) were around. This finding is also in line with Mare et al.'s study, which found that guests considered a motion sensor as a potentially privacy-violating device because it could detect people's movements and calculate how many people are in the room [39].

Other results, however, indicate some inconsistency when compared to the literature. First, both device location and the duration of stay did not significantly impact our participants' comfort level or their privacy negotiation intention. On the one hand, this finding is somewhat surprising since both factors are often associated with the amount of data collection (e.g., more data can be collected overall longer stays) and the sensitivity of collected data (e.g., data collected in a bedroom is generally considered more sensitive than in the hallway), which may further influence people's privacy perceptions [19, 29, 65]. On the other hand, however, such a finding is also somewhat reasonable because in our study, our participants were considered bystanders in Airbnb rentals. Literature has suggested that bystanders often have different privacy perceptions and priorities when around smart home devices or other devices that may collect data, resulting in different behaviors [1, 12, 19, 42, 55, 61, 67]. For example, even if bystanders have privacy needs, they may choose not to act on it considering other social factors, such as the potential for social confrontation, power dynamics [12, 19, 61]. Additionally, bystanders generally lack further necessary knowledge or information to determine the purpose of other people's smart home devices and data practices [41]. In our study, even though we did not explicitly ask our participants to consider themselves as bystanders, our data still suggested that most participants held a *bystander mindset* when responding to the survey, e.g., participants believed that they did not own the device and did not have knowledge of the device purpose or data practices. Furthermore, compared to other environments (e.g., at a friend's house), Airbnb presents different dynamics (e.g., payment is involved in the host-tenant relationship) and priorities (e.g., price, location). This bystander mindset and the unique environment in Airbnb may further influence how our participants perceived their privacy in an Airbnb rental, their privacy expectations, and their negotiation intention. As a result, device location impacted their privacy perceptions

less than other factors we studied, such as the data types and social relationships.

Our paper also suggested that people preferred asynchronous channels of communication (i.e., text messages, emails) over synchronous communication (i.e., phone calls, face-to-face) even though the latter is often better for negotiation. There could be multiple reasons for this finding, some of which may be unrelated to the negotiation process and its effectiveness. One reason could be that participants may find it more convenient to negotiate via text or email, as these asynchronous requests can be sent instantly without having to wait in line on the customer support hotline. As a result, asynchronous communication may actually become the more effective option. Furthermore, participants may find additional value when using asynchronous communications, as text or emails typically leave records that can be saved for future use (e.g., in the court). Finally, participants consider messaging Airbnb asynchronously as companies often offer live online chat services to support such needs. In many cases, Airbnb hosts may also respond promptly, especially at the time of tenant check-ins.

5.3 Design Implications

Based on our findings, we draw the design implications for both Airbnb and the hosts.

5.3.1 Implications for Airbnb

Enforcing disclosure of data collection. As a home-sharing platform, Airbnb already requires hosts to disclose their rental information and details of their services, including the types of smart home devices installed in the property [2, 3]. However, the Airbnb website only includes a subset of smart devices for hosts to check, including smart TV, smart air conditioning, and smart smoke alarm [2]. In addition, the existing policies do not require disclosure of the data practices of these smart home devices. We suggest that Airbnb should expand the selection of smart home device types on the setup page, and at the same time, require hosts to disclose the data practices associated with their devices because most participants in our study would like to learn not only the types of devices that are included in the rental but also their purposes, data collection, and how the collected data will be handled.

Standardized template to disclose data practices of smart devices. We acknowledge that, in some cases, the hosts who installed the smart devices are unaware of their data practices. As such, we suggest that Airbnb should formulate standardized templates to facilitate data practice disclosure and embed these templates in the setup page. One concrete idea is to adopt privacy labels (similar to Apple's Privacy Label systems in the most recent iOS [7]). Airbnb may further develop privacy label templates for different types of smart devices, whereby the data practices will be pre-populated based on the device types (similar to the Internet of Things Privacy Infrastructure [25]). Tenants may also benefit from the standardized template as users generally have a better understanding of such labels [24, 34, 35].

Developing mechanisms to support privacy negotiation. From a platform perspective, Airbnb is uniquely positioned to support privacy negotiations between hosts and tenants. One concrete idea is to build the negotiation feature on the host's setup page. Hosts can decide whether to allow negotiation on individual smart devices or not. If allowed, tenants will be able to indicate their preferences at the time of booking (e.g., requesting the security camera to be turned off during their stay). Airbnb should also provide tenants feedback on whether the hosts have honored their requests or not.

5.3.2 Implications for Airbnb hosts

Disclosing data practices proactively. We suggest that hosts may take some proactive actions to inform their tenants of the devices and their data practices. For example, our results showed that physical signs and paper documents were welcomed by our participants. Hosts may consider setting up physical signs next to any smart devices to indicate their presence, thus allowing tenants to learn more about those devices. Ultimately, for tenants to take action to protect themselves, they should first be aware of the nearby devices and data practices.

Providing instructions of safely operating smart devices. As many participants have indicated that they might take actions by themselves without reaching out to the hosts or other entities, we suggest that hosts may consider providing instructions for tenants to explain whether they are allowed to take (certain) actions on their own and if so, how to safely take actions (e.g., turning off smart devices, adjusting their settings, etc.). Hosts may also provide additional materials, such as a physical cover to cover up the security cameras. This is to ensure that tenants will not take aggressive actions by themselves and damage the devices due to inappropriate operation.

6 Conclusion

In this study, we conducted a fully factorial vignette study with 867 participants to explore how to support privacy negotiation between tenants and hosts in Airbnb that are equipped with smart home devices. Our results suggested that device types remained the only factor that had a significant impact on our participants' comfort level and privacy negotiation intention in Airbnb. We further examined our participants' negotiation preferences in terms of with whom, when, how, and why they negotiate. Our study contributes to the growing body of literature on resolving the privacy tension among different stakeholders in smart home environments and points to a promising solution through privacy negotiation.

7 Acknowledgement

We thank all the anonymous reviewers and shepherds for the valuable feedback. This work is supported by National Science Foundation CNS-2232653.

References

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–28, 2020.

[2] Airbnb. Informing guests about security devices, September 2022.

[3] Airbnb. Use of cameras and recording devices, September 2022.

[4] Airbnb. What's expected of guests, September 2022.

[5] Abdulmajeed Alqhatani and Heather Lipford. Exploring parents' security and privacy concerns and practices. Technical report, EasyChair, 2018.

[6] 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. *Proceedings on Privacy Enhancing Technologies*, 3:99–119, 2022.

[7] Apple. Privacy labels. https://www.apple.com/privacy/labels/.

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

[9] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):1–23, 2018.

[10] Natã Miccael Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. " what if?" predicting individual users' smart home privacy preferences and their changes. *Proc. Priv. Enhancing Technol.*, 2019(4):211–231, 2019.

[11] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. Balancing power dynamics in smart homes: Nannies' perspectives on how cameras reflect and affect relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 687–706, 2022.

[12] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. Bystanders' privacy: The perspectives of nannies on smart home surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.

[13] Julia Bernd, Alisa Frik, Maritza Johnson, and Nathan Malkin. Smart home bystanders: Further complexifying a complex context. In *Proceedings of the 2nd Symposium on Applications of Contextual Integrity*, 2019.

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

[15] Hongliang Chen and David Atkin. Understanding third-person perception about internet privacy risks. *New Media & Society*, 23(3):419–437, 2021.

[16] Shijiao Joseph Chen, Kuttimani Tamilmani, Khai Trieu Tran, Donia Waseem, and Vishanth Weerakkody. How privacy practices affect customer commitment in the sharing economy: A study of airbnb through an institutional perspective. *Industrial Marketing Management*, 107:161–175, 2022.

[17] Hui-Lien Chou and Chien Chou. How teens negotiate privacy on social media proactively and reactively. *New Media & Society*, page 14614448211018797, 2021.

[18] Rune Haubo B Christensen. Cumulative link models for ordinal regression with the r package ordinal. *Submitted in J. Stat. Software*, 35, 2018.

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

[20] DailyMail. Shocking video shows house guests trash an airbnb rental during an all-out brawl in dallas, September 2022.

[21] Ralf De Wolf. Contextualizing how teens manage personal and interpersonal privacy on social media. *New media & society*, 22(6):1058–1075, 2020.

[22] Rajib Dey, Sayma Sultana, Afsaneh Razi, and Pamela J Wisniewski. Exploring smart home device use by airbnb hosts. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–8, 2020.

[23] David D'Acunto, Serena Volo, and Raffaele Filieri. "most americans like their privacy." exploring privacy concerns through us guests' reviews. *International Journal of Contemporary Hospitality Management*, 2021.

[24] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 447–464. IEEE, 2020.

[25] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2021.

[26] Tomas Gecevicius, Yaliang Chuang, and Jingrui An. Smart arbnb: Smart home interface for airbnb with augmented reality and visible light communication. In *CHIIoT@ EWSN/EICS*, 2021.

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

[28] Joseph K Goodman and Scott Wright. Mturk and online panel research: The impact of covid-19, bots, tiktok, and other contemporary developments. 2022.

[29] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). In *USENIX Security Symposium*, pages 255–272, 2018.

[30] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. Amazon vs. my brother: How users of shared smart speakers perceive and cope with privacy risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[31] William Jang, Adil Chhabra, and Aarathi Prasad. Enabling multi-user controls in smart home devices. In *Proceedings of the 2017 workshop on internet of things security and privacy*, pages 49–54, 2017.

[32] Li Jiang, Da-You Liu, and Bo Yang. Smart home research. In *Proceedings of 2004 international conference on machine learning and cybernetics (IEEE Cat. No. 04EX826)*, volume 2, pages 659–663. IEEE, 2004.

[33] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I Hong. Exploring the needs of users for supporting privacy-protective behaviors in smart homes. In *CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2022.

[34] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[35] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, pages 1573–1582, 2010.

[36] Evan Lafontaine, Aafaq Sabir, and Anupam Das. Understanding people's attitude and concerns towards adopting iot devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–10, 2021.

[37] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I Hong. Understanding challenges for developers to create accurate privacy nutrition labels. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2022.

[38] Heather Richter Lipford, Madiha Tabassum, Paritosh Bahirat, Yaxing Yao, and Bart P Knijnenburg. Privacy and the internet of things. *Modern Socio-Technical Perspectives on Privacy*, page 233, 2022.

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

[40] Karola Marky, Nina Gerber, Michelle Gabriela Pelzer, Mohamed Khamis, and Max Mühlhäuser. "you offer privacy like you offer tea": Investigating mechanisms for improving guest privacy in iot-equipped households. *Proceedings on Privacy Enhancing Technologies*, 4:400–420, 2022.

[41] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. "you just can't know about everything": Privacy perceptions of smart home visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*, pages 83–95, 2020.

[42] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. " i don't know how to protect myself": Understanding privacy perceptions resulting from the presence of bystanders in smart environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, pages 1–11, 2020.

[43] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), nov 2019.

[44] Tanya McGill and Nik Thompson. Gender differences in information security perceptions and behaviour. 2018.

[45] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. Toys that listen: A study of parents, children, and internet-connected toys. In *Proceedings of the 2017 CHI conference on human factors in computing systems*, pages 5197–5207, 2017.

[46] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an {IoT} world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, 2017.

[47] NZHerald. Christchurch airbnb party fatal stabbing: Property owners 'devastated', September 2022.

[48] Vincent N Parrillo and Christopher Donoghue. Updating the bogardus social distance studies: A new national survey. *The Social Science Journal*, 42(2):257–271, 2005.

[49] Aarathi Prasad, Ruben Ruiz, and Timothy Stablein. Understanding parents' concerns with smart device usage in the home. In *International Conference on Human-Computer Interaction*, pages 176–190. Springer, 2019.

[50] Giulia Ranzini, Michael Etter, and Ivar Vermeulen. My home on the platform: exploring the physical privacy concerns of home-sharing providers. *International Journal of Hospitality Management*, 86:102433, 2020.

[51] Amit Kumar Sikder, Leonardo Babun, Z Berkay Celik, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A Selcuk Uluagac. Who's controlling my device? multi-user multi-device-aware access control system for shared smart home environment. *ACM Transactions on Internet of Things*, 2022.

[52] Teodor Sommestad, Henrik Karlzén, and Jonas Hallberg. A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP)*, 9(1):26–46, 2015.

[53] Jose M Such and Michael Rovatsos. Privacy policy negotiation in social media. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 11(1):1–29, 2016.

[54] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. 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*, pages 1–12, 2020.

[55] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. "it would probably turn into a social faux-pas": Users' and bystanders' preferences of privacy awareness mechanisms in smart homes. In *CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2022.

[56] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 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*, pages 129–139, 2014.

[57] Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I Hong, and John Zimmerman. Are you close with me? are you nearby? investigating social groups, closeness, and willingness to share. In *Proceedings of the 13th international conference on Ubiquitous computing*, pages 197–206, 2011.

[58] Wiktoria Wilkowska and Martina Ziefle. Privacy and data security in e-health: Requirements from the user's perspective. *Health informatics journal*, 18(3):191–201, 2012.

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

[60] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*, pages 1–12, 2019.

[61] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–24, 2019.

[62] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. Privacy mechanisms for drones: Perceptions of drone controllers and bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6777–6788, 2017.

[63] Seounmi Youn. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs*, 43(3):389–418, 2009.

[64] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, 2017.

[65] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *USENIX Security Symposium*, pages 159–176, 2019.

[66] Bo Zhao. Unraveling home protection in the iot age: Smart living, mixed reality, and home 2.0. *Colum. Sci. & Tech. L. Rev.*, 21:1, 2019.

[67] Yuhang Zhao, Yaxing Yao, Jiaru Fu, and Nihan Zhou. " if sighted people know, i should be able to know:" privacy perceptions of bystanders with visual impairments around camera-based technology. *arXiv preprint arXiv:2210.12232*, 2022.

[68] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–20, 2018.

8 Appendix

8.1 Screening Survey Question

Q1 When was your most recent stay in an Airbnb property?
- Past three days
- Past week
- Past month
- Past six months
- Past year
- I have never stayed in Airbnb before.

8.2 Main Survey

Experiences with smart home devices

Q1 Which of the following devices do you own or regularly use? (Select all that apply)
- Smart Remote Controls (e.g., Samsung SmartThings Hub)
- Smart Lighting Solutions (e.g., Samsung SmartThings Hub, Philips Hue),
- Smart Voice-Activated Products (e.g., Amazon Echo, Apple Home),
- Smart Door Locks (e.g., Yale Assure Lock, Honeywell Smart Locks)
- Smart Toys (e.g., iDog, Sphero Mini, Makey Makey)
- Smart Home Appliances (e.g., LG Smart ThinQ Washer/Dryer /Refrigerator Samsung)
- Smart Home Sensors (e.g., Hue Motion Sensor, Samsung SmartThings, OxyLED)
- Smart Home Utilities (e.g..Nest Learning Thermostat, Blossom Smart Watering Controller)
- Smart Window Solutions (e.g., Smart Tint, Smart Door and Window Sensors)
- Smart Home Surveillance Cameras (e.g., Arlo Smart Camera, Nest Indoor Cam)
- I do not use smart home devices regularly
- Other (open-ended question)

Q2 How long have you been using smart home devices?
- Less than 3 months
- Between 3 months - 1 year
- More than 1 year

Q3 In general, how comfortable or uncomfortable are you with the data collection by smart home devices?
- Very comfortable
- Somewhat comfortable
- Somewhat uncomfortable
- Very uncomfortable

Scenario-based Questions

*Imagine the following scenario: you are staying an Airbnb alone for **duration of stay** and the **device type** present in the **device location** is collecting your data. Please answer the following questions based on this scenario.*

Q4 How comfortable or uncomfortable are you with the data collection in this scenario?
- Very comfortable
- Somewhat comfortable
- Somewhat uncomfortable
- Very uncomfortable

Q5 In this scenario, which of the following strategies will you use when you discover the smart device usage and their data practices? (Select all that apply)
- Take actions on your own (e.g., to unplug the smart homes)
- Communicate your needs with someone
- Post your experiences on social media (e.g., Twitter/Facebook/other platforms)
- Report to law enforcement agencies
- Report to Airbnb
- Leave Airbnb
- Do nothing
- Others

Q6 In this scenario, how likely or unlikely would you communicate and discuss (i.e., negotiate) your preferences with someone when you discover the smart device usage and their data practices?
- Very likely
- Somewhat likely
- Somewhat unlikely
- Very unlikely

Q7 How likely or unlikely will you communicate and discuss (i.e., negotiate) your concerns with the following parties? (Participants were asked to rate each incident on a 4-point scale: Very likely ,Somewhat likely, Somewhat unlikely, and Very unlikely)
- Airbnb host
- Airbnb
- Law enforcement agency
- Third-party (e.g., Consumer Report)
- Smart home device manufacturer
- Other

Q8 Can you briefly explain why?

Q9 What goals do you aim to achieve from such communication (or negotiation) in this scenario?

Q10 How would you like to communicate and discuss (i.e., negotiate)? (Select all that apply)
- Send messages to host through Airbnb mobile app
- Send emails to host
- Call host
- Send emails to Airbnb customer service
- Call Airbnb customer service
- I will leave a review on the Airbnb website
- Send emails to the manufacturer
- Use services from Third-party
- Communicating face-to-face with the host
- Other

Q11 When would you prefer to communicate and discuss (i.e., negotiate)?
- On the application while booking
- At the property during check-in
- During check-out
- None
- Other

Q12 Who do you think should be responsible for implementing your preferences?

- Airbnb Guest
- Airbnb Host
- Airbnb
- Law enforcement agency
- Smart home device manufacturer
- Third-party
- Other

Hypothetical travel companion

Referring to the above scenario. Instead of going alone, you are traveling with **(one of "close relatives", "close friends", "colleagues in the same organization", "people in the same occupation", "domestic strangers", "someone you don't know")**, will this increase or decrease your intention learn about the smart devices and their data practices in this scenario? Please briefly explain why.

Q14 Will this increase or decrease your intention to communicate and discuss (i.e., negotiate) your preferences with someone when you discover the smart device usage and their data practices? Please briefly explain why.

Demographic Questions

Q15 How do you describe yourself?

- Male
- Female
- Non-binary

Q16 How old are you?

- 18-24 years old
- 25-34 years old
- 35-44 years old
- 45-54 years old
- 55+ years old

Q17 What is your highest education level?

- High school or below
- Bachelor degree
- Master degree
- Doctoral degree
- Prefer not to answer

Q18 Please select the statement that best describes your comfort level with computing technology.

- Ultra Nerd: I build my own computers- run my own servers- code my own apps. I'm basically Mr. Robot.
- Technically Savvy: I know my way around a computer pretty well. When anyone in my family needs technical help- I'm the one they call.
- Average User: I know enough to get by.
- Luddite: Technology scares me! I only use it when I have to.

Q19 What best describes your employment status over the last three months?

- Working full-time
- Working part-time
- Unemployed and looking for work
- A homemaker or stay-at-home parent
- Student
- Retired
- Other

Q20 What is your current marital status?

- Married
- Living with a partner
- Widowed
- Divorced/Separated
- Never been married