Well-intended but half-hearted: Hosts' consideration of guests' privacy using smart devices on rental properties

Sunyup Park, *University of Maryland, College Park;* Weijia He, *Dartmouth College;*
Elmira Deldari, *University of Maryland, Baltimore County;*
Pardis Emami-Naeini, *Duke University;* Danny Yuxing Huang, *New York University;*
Jessica Vitak, *University of Maryland, College Park;* Yaxing Yao, *Virginia Tech;*
Michael Zimmer, *Marquette University*

https://www.usenix.org/conference/soups2024/presentation/park

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

Open access to the Proceedings of the Twentieth Symposium on Usable Privacy and Security is sponsored by USENIX.

Well-intended but half-hearted: Hosts' consideration of guests' privacy using smart devices on rental properties

Sunyup Park
Univ. of Maryland, College Park

Weijia He
Dartmouth College

Elmira Deldari
Univ. of Maryland, Baltimore County

Pardis Emami-Naeini
Duke University

Danny Yuxing Huang
New York University

Jessica Vitak
Univ. of Maryland, College Park

Yaxing Yao
Virginia Tech

Michael Zimmer
Marquette University

Abstract

The increased use of smart home devices (SHDs) on short-term rental (STR) properties raises privacy concerns for guests. While previous literature identifies guests' privacy concerns and the need to negotiate guests' privacy preferences with hosts, there is a lack of research from the hosts' perspectives. This paper investigates if and how hosts consider guests' privacy when using their SHDs on their STRs, to understand hosts' willingness to accommodate guests' privacy concerns, a starting point for negotiation. We conducted online interviews with 15 STR hosts (e.g., Airbnb/Vrbo), finding that they generally use, manage, and disclose their SHDs in ways that protect guests' privacy. However, hosts' practices fell short of their intentions because of competing needs and goals (i.e., protecting their property versus protecting guests' privacy). Findings also highlight that hosts do not have proper support from the platforms on how to navigate these competing goals. Therefore, we discuss how to improve platforms' guidelines/policies to prevent and resolve conflicts with guests and measures to increase engagement from both sides to set ground for negotiation.

1 Introduction

Digital platform mediated short-term rentals (STRs), such as Airbnb and Vrbo, have become increasingly popular over the last decade. With the popularity and diversity of smart home devices (SHDs), STR hosts are increasingly using SHDs to add convenience for guests and to monitor the property's and guests' safety remotely [3,12,41,55,57]. The increased use of SHDs in STRs, however, raises privacy concerns that ranges from interpersonal entities' monitoring and surveillance, to people's data being collected, stored, and shared with institutional entities such as device manufacturers, law enforcement, and third-parties [9, 13, 15, 27, 30, 35, 36, 45, 54, 55].

Research has shown that Airbnb guests are uncomfortable with devices that could potentially monitor them [36, 54]. In fact, STRs guests may have unique privacy expectations, especially when compared to those in traditional hotels. STRs provide an unique "feeling of home" to its customers [63], and people expect greater privacy at homes than any other places [16]. Therefore, guests may have greater expectations of privacy in STRs than in hotels. Additionally, STRs are generally managed by individuals (e.g., hosts) rather than corporations, indicating a possible transfer of legal responsibility [**?**], which may further enhance guests' privacy concerns.

Meanwhile, Airbnb hosts express little or no concern about guests' privacy when using SHDs on their property [15]; rather, their concerns about privacy pertained to guests accessing hosts' data. At the same time, STR hosts are incentivized to accommodate guests' privacy expectations to ensure their positive experience. One way to do this is for guests to negotiate their privacy needs with hosts [54] and address any tension between hosts' goals of using SHDs and guests' values of privacy. What is not clear, however, is whether hosts feel willing and able to engage in such negotiation.

In this paper, we focus on investigating hosts' perspective on if and how they negotiate privacy with guests. Privacy negotiation involves multiple stakeholders trying to reach a consensus regarding data collection practices [54]. Majority of prior work focuses on guests' privacy needs [36,54]. While Dey et al. [15] explored Airbnb hosts' motivation to use SHDs, we still lack knowledge about hosts' current practices around SHD usage, especially in terms of managing [1] and disclosing SHDs. Therefore, we ask the following research questions:

RQ1: How do short-term rental (STR) hosts use smart home devices (SHDs) in their rental properties?

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

[1] In this paper, we define smart home device management as managing accounts, reviewing and deleting data, and granting control of devices.

RQ2: How do STR hosts manage SHDs on their properties?
RQ3: How do STR hosts communicate about their SHDs with guests?

To answer our research questions, we conducted an exploratory interview study with 15 STR hosts (e.g., Airbnb/Vrbo) about their usage of SHDs on their rental properties, how they manage and communicate with guests about their devices, and how, if at all, they consider guests' privacy when making decisions related to SHDs. Aligning with prior work [15, 36], we found that hosts use SHDs for safety and security purposes, which inevitably monitor their guests. Contrary to prior research [15, 36], however, we found that hosts take guests' privacy into consideration, albeit in limited ways. Hosts consider guests' privacy when deciding which devices to use and where to locate them, logging out of guests' accounts, limiting monitoring and control during guests' visits, and disclosing their devices to guests. We also found that hosts rarely, if ever, review or delete data; they provide limited control options to guests; and they do not disclose all SHDs.

Our paper contributes to the existing literature on privacy negotiation among multiple stakeholders in three key ways:

- We highlight hosts' conflicting needs in protecting their STRs versus protecting guests' privacy.
- We describe hosts' (limited) actions to ease guests' privacy concerns, especially in managing SHDs' data.
- We provide recommendations to improve platforms' policies/guidelines and design features to prevent and facilitate privacy negotiation between hosts and guests.

2 Related Work

2.1 Multi-user interactions in smart homes

A smart home is a multi-user environment that involve primary users and non-primary users (e.g., alternate primary users, secondary users, and guests) based on different roles and usage scenarios [20, 25, 28, 34, 52, 59]. Primary users are those involved in purchasing, installing, using, and managing SHDs [20], while non-primary users are those who are less involved in managing SHDs, but focus on using the SHDs managed by the primary user [28]. Bystanders are an important subset of non-primary users [60], and are users who "happen to" use SHDs (also referred to as "passenger users" by [28] and "incidental users" by [13]). Research has found that when primary and non-primary users have different ideas about privacy [7, 28, 39, 40], there could be tensions and conflicts, such as passengers' concerns about the device purpose and potential surveillance and monitoring [13, 28, 29].

In the short-term rental (STR) context, we consider hosts as primary users because they purchase, install, use, and manage SHDs for their rental properties. Likewise, we consider guests bystanders because they use or are exposed to data collection by SHDs that hosts have in their STRs. However, unlike previous studies that address traditional home setups [13, 28, 52, 59, 60], stakeholders in STRs are based on a transactional relationship, incentivizing negotiation. Guests can always pick a different listing if they are unhappy with the property (e.g., hosts' usage of SHDs), while hosts are motivated to attract more guests. Therefore, it gives guests the power to negotiate, making it an ideal setting to study how people negotiate their privacy preferences.

2.2 Smart rentals and privacy

Privacy is an issue for both hosts and guests in the STR context. For example, hosts are concerned about privacy when their identities are disclosed through their public profiles [50] while guests concerned about smart devices such as hidden cameras, [11, 21, 58], general smart cameras [13, 17, 42], and smart speakers [13]. In fact, Schutte [45] found that guests were less satisfied staying in rental properties with SHDs and identified privacy as one of the reasons.

As one of the most popular STR platforms [49], Airbnb highlights the tension and conficts between hosts and guests. From the hosts' perspective, privacy was rarely considered and if it was, it was about hosts' own privacy (e.g., guests accessing hosts' information through SHDs) [15]. From the guests' perspective, they were concerned about being monitored by SHDs and the lack of control they have with the devices, and thus, had different views on information sharing (e.g., Airbnb hosts wanted to access guests' search history, but guests were uncomfortable with sharing that information) [36]. Even for less privacy-invasive devices (e.g., thermostats), hosts and guests had conflicts about how much control they want and related access to data [35]. Wang et al. [54] further identified specific devices (e.g., security cameras, voice assistants, motion sensors) that made guests uncomfortable and suggested privacy negotiation with hosts as a possible way to lessen guests' privacy concerns.

Our study complements these findings by providing insights into how hosts use their SHDs, including data management and disclosing their devices, and how—if at all—they negotiate with guests regarding SHDs in their properties.

2.3 Smart home device and data management

In theory, smart home users can mitigate their privacy concerns by engaging in privacy-protecting behaviors, such as adjusting the location of the devices [61], avoiding using certain functions [51], receiving notifications [31], or in some cases, avoid purchasing them in the first place [23]. Less intuitive and therefore uncommon is to take technical actions, such as changing passwords and/or using two-factor authentication [51], turning-off microphones, deleting video recordings and/or behavior logs [56]. In fact, Jin et al. [26] reported that less than 1% of their respondents take technical actions to manage their smart speakers. In practice, even

smart home power users find it difficult to engage in technical measures to protect their privacy in smart homes [33]. Other research has also investigated data access and control with institutional entities (e.g., manufacturers, advertisement companies, government) [1, 4, 5] and data-sharing behaviors among interpersonal relationships (e.g., family members, domestic workers, guests) [1, 4, 18, 22, 37, 38].

In the context of STRs, a few studies have investigated ways to mitigate guests' privacy, such as building a smart home interface based on local network instead of cloud-based [19], or using blockchain technology to lessen the privacy threats in home sharing economy [24]. Marky et al. [37] further suggested that guests value the feedback of privacy protection status from the hosts and privacy protection should foster collaboration between guests and hosts. The STR context, especially from the hosts' perspective, is uniquely different from other contexts (e.g., visiting friends) and may introduce new interactions and reactions to SHDs. Our work extends the prior work with an emphasis on the hosts' perspective.

3 Method

To answer our research questions (RQs), we conducted online interviews with 15 short-term rental (STR) hosts (e.g., Airbnb/Vrbo). Our study was approved by the first author's institution's IRB.

3.1 Recruitment

We used a short screening survey to recruit participants based on two criteria: (1) they are currently hosting one or more STR properties, and (2) they are currently using or interested in using smart home devices (SHDs) in their STR properties. We initially targeted Airbnb hosts but faced significant difficulties recruiting them. At the same time, we found out that many people cross-host on Airbnb and Vrbo. Therefore, we decided to expand and recruit Vrbo hosts as well.

Recruiting STR hosts was extremely difficult due to the exclusiveness of the community. We recruited through word-of-mouth, social media, and online groups targeted to Airbnb hosts (e.g., Airhost forum, subreddits for Airbnb hosts, and Facebook groups). After facing recruitment challenges, we additionally recruited through Craigslist, Airbnb host meetups, and posted flyers in Airbnb-dense areas. Finally, we also used a snowballing method to recruit additional participants by asking for referrals, either in their surveys or interviews. We had a total of 139 screener survey respondents. After filtering out bots and invalid STR accounts, we contacted 73 potential participants; 46 replied, and we were able to schedule 15 participants. This sample size is above average (12) for the CHI community [8]. In addition, we rigorously validated STR hosts by (1) asking for their STR profiles in the survey, (2) sending a private message to their STR profiles to validate their account, and/or (3) matching profile pictures and descriptions with participants' survey response and interview, to ensure our data quality. Participants who completed the interviews were compensated with a US$50 gift card. Participants who introduced other participants were compensated with an additional referral fee (USD1 per referral).

3.2 Data collection

Data collection started in August, 2023 until January, 2024. We conducted two pilot interviews to revise and refine our study protocol. For example, we found that the pilot participant who was interested in using SHDs also provided valuable insights, therefore decided to recruit both hosts who use or are interested in using SHDs (e.g., P2, P12). Pilot interviews are not included in the data analysis.

3.2.1 Interview protocol

Each Zoom interview was recorded. The interviews lasted 52 minutes on average. Interview questions were divided into four sections. First, we provided our definition of SHDs – *household items that are connected to the Internet or a home network to enhance functionality, connectivity, and efficiency within the home*–and asked about their motivations for using SHDs. Second, we asked our participants about their experiences using SHDs on their STRs, focusing on how they manage their devices and if there were any challenges in managing their devices. Third, we asked our participants about their perceptions and practices of disclosing SHDs to guests. We then introduced participants' STR platforms' guidelines and policies regarding SHD disclosure and asked about their familiarity and perceptions. The final set of questions covered various privacy considerations with SHD use. We first asked participants about general concerns related to SHDs and potential issues stakeholders might face. If, until this point, participants did not mention privacy concerns, which was rare, we introduced an example of hosts and guests conflict when using smart speakers. We asked our participants about their thoughts on this situation. We ended our interview by asking participants to brainstorm resolving conflicts around using SHDs from multiple stakeholders' perspectives The interview protocol is provided in appendix A.

3.2.2 Participant information

As shown in Table 1, our participants consist of 13 Airbnb and 2 Vrbo hosts, whose hosting experience, numbers and types of properties, and experiences with SHDs vary. Among SHD users (n=13), the number of devices ranged from two to ten. Our participants ranged from 25 to 65+ years old, and identified as female (n=8) and male (n=7). Most participants identified as white (n=11), and most (n=11) had at least a bachelor's degree.

ID	Age	Gender	Platform	Hosting Time	Types of property	Types of SHDs used (or want to use)	Familiarity with SHDs
P1	25-34	Male	Airbnb	before 2018	primary residence	Speakers/Voice Assistants(VAs), lights, TVs, cameras, alarms	extremely familiar
P2*	65+	Male	Airbnb	since 2022	secondary residence	(Lights, thermostats)	slightly familiar
P3**	45-54	Male	Airbnb	since 2023	investment property	Lights, thermostats, TVs, doorbells, door locks, routers, appliances, switches, alarms	very familiar
P4	35-44	Male	Airbnb	since 2021	secondary residence	Speakers/VAs, thermostats, TVs, door locks, cameras, appliances, garage doors, switches, sensors, alarms	extremely familiar
P5	45-54	Male	Airbnb	since 2022	investment property	TVs, doorbells, door locks	extremely familiar
P6	35-44	Female	Airbnb	since 2021	primary residence	Thermostats, TVs, vacuums, sensors, alarms	moderately familiar
P7	35-44	Male	Airbnb	since 2022	primary residence	Speakers/VAs, switches	moderately familiar
P8	35-44	Female	Airbnb	since 2021	primary residence	Thermostats, TVs, door locks, cameras, routers	extremely familiar
P9	25-34	Male	Airbnb	since 2021	primary residence	TVs, ACs	moderately familiar
P10	65+	Female	Vrbo	before 2018	secondary residence	Speakers/VAs, thermostats, TVs, window solutions	extremely familiar
P11	35-44	Female	Airbnb	since 2020	secondary residence	Speakers/VAs, TVs, door locks, cameras	very familiar
P12*	45-54	Female	Airbnb	before 2018	secondary residence	(Speakers/VAs, lights, thermostats, TVs, doorbells, door locks, cameras, alarms)	moderately familiar
P13	55-64	Female	Vrbo	before 2018	secondary residence	Speakers/VAs, TVs	very familiar
P14	25-34	Female	Airbnb	since 2021	primary residence	Speakers/VAs, thermostats, TVs, vacuums, doorbells, door locks, cameras, switches, sensors, alarms	very familiar
P15	35-44	Female	Airbnb	since 2019	primary residence	TVs, cameras	moderately familiar

* The participant does not have SHDs on their Airbnb property currently but is interested in using them.
** P3's interview was not transcribed because P3's recording was lost. We created a detailed memo of P3's session for analysis and write-up, but we did not quote him anywhere.

Table 1: Participant Information.

3.3 Data analysis

Our recruitment took 6 months in total. To ensure the progress, we analyzed our data alongside data collection. We transcribed the audio recordings using *Rev.ai* and manually cross-checked the transcriptions with the recordings for quality assurance. We then imported the transcriptions into *Atlas.ti* for qualitative coding. P3's recordings were lost due to technical issues. However, we took detailed notes during the interview and used them to validate the themes. Thus, similar to Koshy et al. [28], we did not discard P3 from our study. The three lead authors conducted multiple iterative rounds of coding, following coding guidelines by Saldaña [44]. First, we applied structural coding (i.e., building codes based on the interview protocol) and produced 15 initial codes. Next, we selected three transcripts with rich data and applied open coding based on the initial codes to expand on the codes, producing 50 codes. Last, we distributed the transcripts so that at least two researchers coded each transcript and produced 95 final codes. During this process, we met multiple times to resolve any disagreements and reach consensus on codes. The final codebook is provided in appendix B.

Data collection continued until we determined saturation had been achieved; upon hearing no new attitudes or experiences in our final two interviews, we determined that additional data collection was unlikely to yield additional insights [32]. After coding all transcripts, we selected codes that were relevant to answering our RQs and conducted thematic analysis of each, generating analytic memos [44]. The selected codes for each RQ are:

RQ1: STR property description, types and location of SHDs, motivations for using or not using SHDs, reasons for device purchase and usage.

RQ2: SHD management (accounts, access, manual operations), (dis)advantages of using SHDs (confusion, complications, failures).

RQ3: Codes related to STR guidelines/policies (familiarity, perceptions, needs/wants), disclosure practices (perceptions, considerations, preferences) and resolving conflicts (potential conflicts, willingness to negotiate).

Given the qualitative nature of this paper, we refrain from reporting the exact number of participants for each theme. Instead, we use the following terminologies when reporting our results: few (0-25%), some (25-45%), about half (45-55%), many/most (55-75%), and almost all (75-100%). This is similar to other qualitative studies (e.g., [7, 16, 62, 64]).

3.4 Limitations

We faced significant challenges recruiting STR hosts, partially because we aimed to verify that our participants were actual hosts. Therefore, although we have limited participant numbers and diversity, we were able to capture real hosts' experiences. Social desirability bias [6] can happen in interview studies. We tried mitigating them by avoiding using languages related to privacy during recruitment and mentioning privacy before participants mentioned it. Instead, we prompted our

participants to think about privacy by asking the benefits and drawbacks of using SHDs on their STRs or introducing a situation where conflicts can arise between the host and the guest because of privacy concerns.

4 Findings

This section is organized based on our three research questions, which cover hosts' smart home device (SHD) usage practices in their short-term rentals (STRs), their device management practices, and how they communicate with guests regarding SHDs.

4.1 Hosts' usage of smart home devices

4.1.1 Types and locations of SHDs

Figure 1 shows the types and locations of SHDs used (or wanted to use) by hosts. Smart thermostats and smart speakers ($n = 10$) were the most frequently used (or wanted to use), followed by streaming devices, smart cameras, and smart door locks ($n = 9$). These devices were located in various spaces in the property, spanning from private spaces (i.e., guests only) to shared spaces (i.e., hosts and guests) to public spaces.

Guests' private spaces can range from a private room in a shared property to an entire property and include spaces such as the bedroom, living room, and the kitchen. Private spaces had the most SHDs, with entertainment devices such as smart speakers and smart TVs being most popular. Smart cameras, on the other hand, were rarely placed in guests' private spaces, which is in line with the recent update to Airbnb's guidelines banning indoor cameras [43]. Smart thermostats and smart alarms were placed in shared spaces where both hosts and guests have access. These devices were often considered as less-privacy invasive. SHDs for safety and security purposes (e.g., smart door locks, smart cameras) were placed in public spaces (e.g., front/back doors, yard).

The majority of our participants' STRs was either their primary or secondary residence, with only two participants explicitly identifying their property as an investment. Interestingly, participants whose STRs were secondary or an investment were more willing to incorporate SHDs than those whose STRs were their primary residence. This strategic approach to adopting SHDs on their property was aimed at enhancing property safety and security through remote control, particularly for hosts who lived far from the property.

4.1.2 Motivations for using SHDs in STRs

One of the main reasons our participants use SHDs on their STRs was to monitor their properties and guests to ensure security and safety. This was especially important for participants whose rental property was not their primary residence and, therefore, needed to use SHDs to manage their properties remotely. These participants used their smartphone apps to control the devices (e.g., door locks, lights, thermostats) on the property remotely, reducing the need to be physically onsite. For example, smart cameras, doorbells, and door locks were used to ensure the number of guests was correct, given that guests often bring more people. P4 stated, *"sometimes people will show up and bring 10 more guests than they said they were going to bring, so we have some security cameras."* Among the devices used for monitoring, our participants were most cautious about using smart cameras, especially where they placed them. P1 stated, *"So for the camera, I think that's the most invasive smart home device that we have. It was important to me to put it somewhere where it's only, where its main function as a security device is most clearly limited. So that's why it faces the front door. And is only triggered when the front door opens, or when there's activity at the front door."* Some of our participants, unfortunately, experienced theft, damage, and other violations of house rules (e.g., smoking) and decided to place smart cameras indoors. P11 placed a smart camera in her living room, stating, *"I'm not sure if it's fine or not, but it's just, it's my property, and it, there are things that are very expensive, and as much as they could pay for it, there's a lot of effort that it takes getting the stuff back again and put it in place."* Our study was conducted before Airbnb updated its guidelines to ban indoor cameras.

4.1.3 Reasons hosts *don't* use SHDs in rental properties

While SHDs were widely used, some participants also explicitly highlighted reasons why they avoided certain devices.

The primary concern revolves around the potential violation of guests' privacy, which could hinder their comfort during their stay at the rental property. Participants emphasized their reluctance to monitor guests inside the property (e.g., avoiding using smart cameras in private spaces). For example, P8 stated, *"I would never put one [smart cameras] inside, obviously, like you'd get kicked off the platform as, and it's super creepy."* Additionally, participants expressed concerns about potential privacy breaches and discomfort for guests. They worried that smart speakers might encroach on guests' privacy by listening to conversations and raised concerns about data collection by these devices. For instance, P8 stated: *"I wouldn't use one of those [smart speakers and voice assistance] in my unit probably because of audio recording. Um, and I think that's kind of what I was hinting at earlier about like tablets or speakers or whatever they are that, um, do record. I'm, I probably side with a guest on that."* In this case, hosts' threat model includes manufacturers and companies accessing guests' data. However, hosts themselves can also be a threat, for example, using "drop in" modes to listen to guests [2]. In the next section(section 4.2.3), we elaborate more on those cases where the host could threaten guests' privacy when using SHDs.

Technical difficulties and the cost of the devices are other

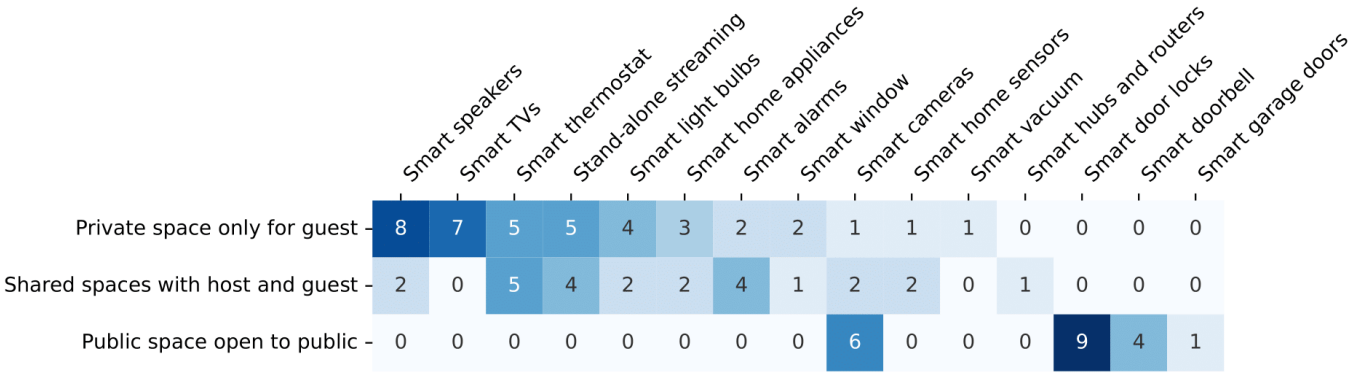

Figure 1: Types and locations of SHDs used by hosts. Private spaces are those areas accessible only to guests. Shared spaces refer to locations utilized by both guests and hosts. Public spaces are areas accessible to the general public.

reasons for not using certain SHDs on the property, as some participants express challenges in installing devices like security cameras or smart door locks. As P7 mentioned, *"Plus the costs, I mean, you have to consider how much it costs to, to do it. Um, and if say the lock gets broken or whatever gets broken or smashed, you know, it's more expensive to replace."*

4.2 Hosts' management of smart home devices

Hosts have access to data generated by guests with SHDs in STRs. We found hosts' lack of care accessing data, retention of data, and sharing data with SHDs. Hosts generally do not share data access with guests, but may do so with others (e.g., property managers); review data on their discretion; rarely delete data. Furthermore, our participants' data management falls short from their intentions to protect guests' privacy; they either are unaware or nonchalant about the privacy and security implications of their devices and data.

4.2.1 Who has access to SHDs' data?

Using hosts' accounts for SHDs in STRs. In general, SHDs need an account to access and control the devices and data. About half of our participants explicitly mentioned that they use their own accounts for their SHDs, which makes them the only ones who can access data collected by the SHDs. One common reason for using their own accounts is to provide a seamless experience for the guests. For example, P11 stated, *"[I use] my account. It's already very hard. Like people are traveling. It is already hard for them to kind of notice this. So as to make these changes. So I just logged them into my account."* Another reason is the complexity and trouble involved in adding a new user and removing them later. As stated by P14, *"you can adjust that [a smart home device] with your phone, but the guests don't have that on their phone... It's hard for the guests to have access to the smart devices 'cause they don't have my phone."*

Privacy and security implications when using guests' accounts for SHDs. Some of our participants reported that guests use their own accounts for the smart TVs and leave their accounts after they leave. This can result in privacy and security breaches, for example, hosts changing guests' account settings or viewing guests' browsing history [36]. Some participants admitted that they do not check if the accounts are logged in with guests' accounts. When this indeed happened, our participants reset or logged out of guests' accounts from the devices. P6 stated, *"we definitely actually reset them [smart TVs] for the next guest every time, because most of the time people forget to reset, like get out of the smart device."* However, P6 also mentioned that most guests do not care to ask to log out of their accounts.

Hosts may share data access with other stakeholders. Several participants mentioned various people who help them with their rental property, including cleaners, caretakers, property managers, and even neighbors. A few granted access/control of SHDs to their property managers to perform their duties more conveniently. For example, P2 stated, *"Yeah, [I will] give her full power over the thermostats because if she forgets to turn it down, and she goes home, she could just do it then."* P10, on the other hand, is a co-host and helps manage someone else's property. She mentioned that she has full access to the property owner's SHDs: *"I have complete access to everything, all of her, her passwords, etc., to work all of the smart devices."* These data management practices will be elaborated further in (section 4.2.3).

4.2.2 Managing control

Our participants wanted to control their SHDs in a way that respects guests' autonomy. Most participants only control their devices before and/or after guests' stay to take care of their properties (e.g., adjusting temperature).

Our participants noted that *"guest mode"* was an effective way to provide guests with the ability to control SHDs. For

example, almost all smart door lock owners created a guest-specific passcode to enter the property. P10 stated, *"I will also provide them with a code for the apartment door. And that I would send that to them, uh, two days before."* A few participants had smart TVs that also supported this feature, allowing hosts to set a guest profile. For devices that do not support guest modes, a few expressed concern about guests' accessing their information or abusing the access, a similar worry was reported in [15]. P7 stated, *"they [guests] could accidentally or intentionally do some, or like, 'Alexa, what are my last five orders?'...and get some kind information outta you."*

Although most participants wanted to make the guests comfortable, some of our participants wanted to have the ability to "override" guests' control. For example, P2 stated, *"if they [guests] turn the heat up to 90 degrees in the winter, I might be inclined to push it back down."*

4.2.3 Hosts' data management practices

In addition to who has access to the data, we were also interested in understanding how hosts manage the data collected by SHDs. We mainly considered two aspects of data management, which are reviewing and deleting data.

Reviewing data. Our participants monitored their smart cameras to make sure that guests have arrived and did not bring additional guests/pets. Unfortunately, unexpected guests/pets were a concern to many hosts, as they worry about insurance violation requirements, fire codes, or building's policies regarding guests. P11 voiced such frustration among many others, *"I don't know what for why, but for Airbnb, a lot of people organize parties, and that's not allowed in my Airbnb, nor in the condominium. It's forbidden. And so that's the reason why I have the cameras."* Some others also mentioned that they would check the camera to ensure the guests had left. P15 told us, *"And then time's like I know that the guest has checked out, so now that I can like begin cleaning."*

During guests' stay, our participants reported reviewing the data if they knew something went wrong. For example, P4 set up various notifications for events related to property damage (e.g., water sensor for flooding, sensors on oven for fire, unreasonable temperature settings). However, other participants relied on their gut feeling when monitoring guests. P11 stated, *"someone told me [he] didn't know how to use the espresso machine, which was a little weird because it was very simple...I didn't have a very good vibe about this guy. I saw him through the camera, and he was kind of pushing it like this. I'm like, oh my gosh, you're gonna break it."* Similarly, P10 mentioned he *"happened to check"* and noticed *"they [the guests] opened the door at some point, and then for like four or five hours, it wasn't closed. It wasn't locked."*

Deleting data. Our participants did not proactively delete data collected from their SHDs. A few reported that they did not delete video data collected from their smart cameras but instead relied on the devices' default expiration. For example, P1 stated, *"that is subject to Simplisafe's system. It gets deleted after 30 days or something."* P14, who owns a Blink camera, also mentioned something similar, but the duration of footage storage can be customized.

A few participants were reluctant to delete data because they needed the data for proof of business. P11 stated, *"you're supposed to tell Airbnb after 14 days, if any incident happened. So even if you try to delete, it's also not a good idea because I'm gonna be asked for stuff like that."* P13 shared a similar concern, stating, *"we don't delete anything that the camera's recording until after the stay. You know, until we know everything went well, the reviews are in all's well, and then we can delete everything."* We also found that few participants were unaware of smart speakers' data collection practices (e.g., access to conversation history).

4.3 Communicating smart home device usage with guests

Negotiating privacy starts with disclosure. Our participants knew and valued disclosing their devices, but also experienced its limitations; cameras were disclosed while other devices were neglected; hosts lacked accountability in disclosing their devices. Nevertheless, hosts viewed disclosure as an effective means to prevent and resolve future conflicts. Due to the lack of guideline, however, hosts' willingness to accommodate guests' privacy concerns were again left to their discretion.

4.3.1 Hosts' perceptions of platforms' guidelines

Both Airbnb and Vrbo have guidelines and policies regarding the use of smart devices on their properties. In summary, both platforms allow devices for security purposes, and only if they are disclosed beforehand. Airbnb, recently banned indoor cameras to respond to increasing concerns of hidden cameras [43]. Vrbo, on the other hand, does not allow any devices indoors unless they cannot be remotely controlled or disclosed, and guests can deactivate them [53]. Vrbo also has brief guidelines on managing data (e.g., limit access and deletion). Details of Airbnb/Vrbo's guidelines/policies regarding smart devices will be discussed in (section 5.3).

Hosts' familiarity with platforms' guidelines. To understand how our participants communicated their SHDs to guests, we first asked about their familiarity with platforms' guidelines/policies regarding the use of smart devices. Some of our participants were familiar with the guidelines/policies and were cognizant of them while setting up and editing their listing on the platform (e.g., through the prompted questions). P1 stated, *"I'm very familiar with them [the guidelines]. I*

knew about it. . . I think from setting up a new listing or editing an existing listing. Airbnb will notify you of fields that are incomplete, and I saw that, through the user interface that I showed you, the safety disclosures field that would allow me to add information about cameras."

Some of our participants who were not familiar with the guidelines/policies thought they were irrelevant to them. For example, P7 stated that since he does not have cameras on the property, *"never really had to look into it."* Similarly, P10 stated, *"we don't have any of the devices that they're talking about."* Too much focus on cameras and recording devices is problematic because, like P7 and P10, hosts can easily neglect to disclose other devices. Further, the definition of recording devices is ambiguous, as multi-function devices (e.g., devices with embedded audio/video) or interconnected devices can also potentially invade guests' privacy.

Notably, a few participants who were unfamiliar with the guidelines/policies thought that they were obvious. For example, P5 stated that although he did not know about the guidelines/policies, he *"kind of know[s] intuitively"*, mentioning that *"you don't want to have cameras inside."* Similarly, P8 stated that she was unfamiliar with the guidelines, but thought that *"the camera is like a requirement to be disclosed in an Airbnb listing"* and that *"if people don't do it, they're failing to follow the guidelines set by Airbnb and just common courtesy in general."* At the time of the study, Airbnb did not ban the use of indoor cameras, which means that there was a mismatch between host expectations and Airbnb requirements.

Hosts' perceptions about platforms' guidelines. About half of our participants were positive about their platforms' guidelines/policies. Our participants thought that they were concise (P7), understandable and reasonable (P13), and useful (P14). For example, P1 thought that it created a norm around the usage of smart devices on rental properties: *"I am glad that Airbnb provides the user interface to have specific disclosures of this because it gets people used to looking for that and, and it helps to create a norm for hosts to disclose any kind of surveillance devices."* Similarly, P4 thought it was a protection for both hosts and guests: *"I think it's a good expectation for renters, for guests to have, and it helps to keep hosts honest, because, you know, a lot of, I've rented from Airbnb, and it's like, half the time the information is wrong, they haven't filled out the stuff right, you know, you get messages from the hosts that are like, definitely for a different property. . . I think it's a protection both for guests and for hosts to have these sorts of policies from Airbnb."*

Some negative sentiments about the guidelines were that they were too generic (P14) or insufficient (P9). For example, P7 thought that the guidelines raised new questions (e.g., if smart doorbells would fit into any category). Similarly, some participants found the definitions unclear and confusing. For example, P9 was confused by the definition of common places (i.e., spaces without sleeping areas) that, *"I don't know if it's generalizable enough for every cases,"* and he preferred that Airbnb should not allow *"anything inside the house."*

Our participants have mixed opinions on what is considered a monitoring or surveillance device. They generally agreed that recording video or audio indoors invades guests' privacy. However, participants also mentioned that the intentions of the devices (P1) or the *"spirit of the device."* (P4) decide whether a device is considered as monitoring or as surveillance. For example, P1 distinguished between cameras and smart speakers in that cameras are generally security devices that are *"intentionally able to be used"* as surveillance devices because of *"how they can be used by the end user."* He added, *"the types of in-the-moment notice that is provided to users around the device whenever the device is listening or cameras are turned on,"* as a reason why smart speakers are not intended to be used to monitor or surveille people. On the other hand, P4 distinguished environmental monitoring (e.g., electricity, humidity) from surveillance, stating that *"the water meter is potentially a monitoring device,"* but *"that's not the spirit of that."*

Hosts' needs/wants in platforms' guidelines. To improve the negative aspects of platforms' guidelines/policies, our participants suggested that platforms need to increase both hosts' and guests' awareness about the existence of smart devices on property.

One way of increasing awareness is educating both hosts and guests to disclose and check whether or not there are smart devices on the property. P8 stated *"a little bit of education"* for both hosts and guests about *"how it [having smart home devices] benefits me [the host] other than just you know, me trying to creep on you [the guest]."*

Another way was to make it mandatory for hosts and guests to disclose and check the devices on the property. P1 pointed out that it is optional for hosts to disclose their devices. *"They [Airbnb] provide[s] that field among all the other fields that they provide when you're filling out a listing description."* Similarly, P4 commented how *"they [Airbnb] could probably do a little bit better job with helping hosts to implement that and to actually put it in front of guests' faces a little bit better."*

Circling back to P1's comment about how disclosing smart devices creates a norm around smart device usage in rental properties, our participants emphasized that this would be a combined effort from the hosts and the guests. P7 delivers this point: *"ultimately I imagine this is not really gonna be a legal thing either. It's just gonna be like a court of public perception. Like if customers demand that this be declared and disclosed, then it will be. And if they don't, then it won't. If enough people stop using Airbnb because people have Google homes, then Airbnb will require hosts to start declaring whether you have something or any kind of listening device."* (P7)

Some participants also suggested design mechanisms within the platform that could create more friction to increase awareness. P4 suggested a *"periodic checking"* from the plat-

forms, considering hosts might add devices after creating their listing. Similarly, P6 wanted notifications from the platform stating *"these are the important stuff. Send this notification to the guest before they arrive."* Furthermore, P16 suggested indicators for hosts (e.g., checkboxes, an asterisk on profile) and filters for guests to look for further information.

4.3.2 Hosts' communication of their SHDs to guests

Disclosing cameras is perceived as necessary. About half of our participants thought that disclosing cameras on the property was necessary. P11 mentioned, *"I think absolutely [disclose] the cameras, because if you don't say about the cameras, you're gonna get in trouble."*

A few participants thought it was crucial to think of disclosing if cameras were located indoors or in private spaces (e.g., bathroom) because they believed that cameras can be used to monitor or surveille guests. For example, P1 stated, *"if they [cameras] were in the guest space, they certainly would need to be disclosed. That could potentially violate Airbnb's policy if it was in a private space, which I guess bathrooms, sleeping areas ... I think the fact that it's able to be manually used as a surveillance device, by which I mean, I can, even though I'm saying it's only turning on if the door is open, I can go into Simplisafe at any time and look through the cameras and record audio and video. So, I think that makes it important to disclose that it's visible, or that it's there."*

In terms of monitoring or surveillance, some participants mentioned that whether or not the devices had recording capabilities was an important factor to consider when disclosing devices. P7 stated, for example, *"I think if it's like recording someone, it would probably be good to notify people."*

Other devices are perceived as unnecessary to disclose. Other than cameras, our participants were unsure or thought it was unnecessary to disclose their smart devices. A few of our participants thought it was unnecessary to disclose smart speakers, which are considered privacy-invasive by guests [36, 54]. P7 mentioned, *"I don't think I would tell anyone that there was an Alexa dot or something in the listing. Both because someone might just go to your home and steal it, but also because, um, they don't really need to know. They could just unplug it if there's a problem."* Similarly, P4 stated that he has a Sonos soundbar with an embedded Google microphone in the living room, but *"don't feel that is a surveillance or monitoring device that would need to be disclosed."*

How hosts disclose their devices. About half of our participants disclosed their smart devices on their rental profiles (e.g., listings, descriptions). Perhaps, the popularity to disclose on their rental profiles was because it was prompted as a default setting when hosts were listing their properties. For example, P1 stated that *"the only steps that we've taken is to use Airbnb built-in disclosure, to disclose the presence of a camera in the home."* These built-in, default disclosures easily provided the hosts to check off the list of devices they have in the property. For example, P14 stated, *"there's a checkbox. Do you have these security devices and devices that are recording? If you check yes, then describe in detail, where is it located?"*

Some participants disclosed their devices at multiple points to ensure guests checked before booking or visiting the place. For example, in addition to disclosing their devices on their profiles, P4 disclosed his devices in his check-in instructions: *"the most important one is the one that we send before people [book]...[the message includes] there are cameras that are facing the two exterior doors."* Similarly, P6 disclosed her devices in the listing and a physical manual *"to make sure they're [guests] gonna do it [read or follow instructions]"* but also acknowledging that *"but most of the time, they're not gonna do it."* P11 shared a similar frustration after disclosing her devices in multiple points, stating *"It's not only on one point, it's on two. If people don't read it, they really need to get their act together, 'cause, I'm already disclosing it twice."*

4.3.3 Hosts' willingness to negotiate with guests

Conflicts with guests around SHDs usage. A few of our participants experienced conflicts with guests around the usage of smart cameras. For example, P5 stated that one of his guests "looked at it [an outdoor smart camera] in an annoying way and then they stopped working". P5 did not respond to it because the guest was considered as a friend. P11, on the other hand, had several disputes with her guests about her cameras. Some guests were upset about her cameras in the living room and tampered them, which P11 reported to Airbnb as property damage. After receiving complaints from her neighbors about her guests making noises late at night, P11 monitored her guests through her cameras in the living room. The guests left a review of her being a predator, and P11 contacted Airbnb to remove those comments. A guest was taken aback when P11 warned the guest leaving trash outdoors with a photo taken from her outdoor camera. At the time of the study, Airbnb allowed cameras indoors, and in her defense, P11 disclosed them. These anecdotes support previous studies' finding about guests' discomfort in using monitoring devices [36, 54], however, also point out that for specific devices (e.g., smart cameras), disclosing might not be sufficient to mitigate guests' concerns.

Most of our participants, however, did not have conflicts around SHDs usage with guests (even for those who had smart cameras). However, they could still anticipate such situations. As a preventative measure, our participants expected platforms to provide a mechanism that ensures hosts disclose their devices and guests to read hosts' disclosure. P8 stated *"they [Airbnb] could potentially make their policy around camera and recording devices a little bit more clear for hosts. I think that some hosts are not, you know, they're*

not super tech savvy. They may not even realize that Amazon Echo records you, so they may not know that's something that should be disclosed," on the caveat that *"some people just may still not care or may not read them."* Some participants, therefore, suggested a mechanism to make sure that guests read the disclosure. P11 stated, *"I think for them [guests] signing a disclosure would be an extra step, and maybe not necessary, but I don't know what else. I mean, they're already consent[ing] by reserving."*

About half of our participants prefer direct communication with the guests if conflicts arise, even with preventative measures. P1 stated, *"I would first expect them [guests] to talk to me about it."* A few of our participants explicitly preferred messaging on the platform because it left them evidence. P6 stated, *"most of the time they [guests] send message to Airbnb and we answer them. This is because if something's happened first of all, Airbnb knows everything. And if they['re] trying to prove anything, you know."*

Hosts' willingness to accommodate guests' concerns Our participants' willingness to accommodate guests' concerns was highly contextual; hosts considered factors such as duration of stay, trust, reasoning, and consequences.

First, a few participants mentioned that the length of the stay or the trust they built with the guests would matter. Contemplating whether he would disable his cameras, P1 stated, *"it would depend on what the guests' concern was related to and the level of trust we'd established with the person, since they are generally long-term roommates. I think if we had a conversation about those concerns, we would consider disabling the security feature, the cameras for security feature in order to help them feel more private and all that."* Similarly, P12 stated, *"if it's a longer stay, I would definitely say we will, we can turn the cameras off at the door and just keep the cameras on at the driveway so we can just monitor who's coming and who's going."*

A few participants also mentioned that they would first seek out the reasons for the requests. P14 stated, *"the security is not just for the guest but it's for myself personally, it's like my home, so I would need to know the reason why first."* A few participants were willing to negotiate, but with the caveat that the guests would be responsible for the consequences. P11 mentioned that *"we can disable the internal camera. I just want you to know that if there's a party and if I get a fee, you're gonna pay the full fee."*

About half of our participants were willing to accommodate guests' privacy concerns by disabling their devices. A few participants were willing to disable their cameras. For example, P1 stated, *"I think we would, depending on what, how that conversation went, I think I would consider disabling it [smart cameras]."*

A few participants stated that they would disable their smart speakers. P9 stated, *"I [will] definitely remove the voice assistant and for the future."* A few participants were willing to disable other devices such as smart TVs, smart outlets, and lights. P7 stated, *"I have a couple smart outlets and um, you can, I can turn the outlets on or off from anywhere so I could turn 'em off and then I don't have to worry about it. Smart lights, you could probably turn to some kind of a dummy mode where they just work like regular lights."*

On the other hand, our participants also had devices that were non-negotiable for various reasons. For a few participants, cameras were a non-negotiable because they were worried about safety and security. P15 stated, *"I think when it comes to like a camera in a public space, it's like, well, what are you planning to do in that public space, let alone in the private space where I don't have a camera... that starts to get really fishy for me."* Other reasons include door locks being necessary to let guests in (P5) and when smart devices are installed and cannot be removed (P11).

5 Discussion

5.1 Concerning usage of smart cameras

Smart cameras were among the top three SHDs that our participants used. Our participants placed these cameras in private, shared, and public places to monitor their properties and guests to ensure safety and security. The ways in which our participants used smart cameras are concerning in many ways, especially considering that guests find the usage of cameras particularly privacy-invading [36, 54].

Our participants' reasons for using smart cameras were to monitor their properties, but by doing so they inevitably, if not intentionally, monitored their guests. For example, our participants place their smart cameras mostly in public spaces (e.g., front door) to count the number of guests arriving, to make sure that guests are bringing the appropriate number of guests. Also, a few participants installed smart cameras in shared spaces after experiencing theft, damage, and other violations of house rules.

At the time of the study, Airbnb allowed indoor cameras, and we had one participant (P11) who placed a camera in a private space (e.g., living room) to monitor guests. Granted, P11 struggled with guests not respecting house rules (e.g., parties) and disclosed upfront to guests about the cameras indoors. However, considering that our participants repeatedly complained that even if they put the effort to disclose SHDs, guests do not care to check, it is unlikely that guests would have known. In addition, when managing devices and data is up to hosts' discretion, monitoring the property can easily creep into monitoring guests. It is indeed a step forward to protecting guests' privacy that Airbnb updated their guidelines to ban indoor cameras, however, there is no accountability to make sure that preexisting cameras are removed from indoors.

Furthermore, the emphasis on smart cameras only opens up new questions: what about multi-function SHDs that have embedded audio/video capabilities? What about interconnected

devices? We touch upon this issue in (section 5.3) when we think about ways to improve platforms' guidelines/policies.

5.2 Hosts' efforts to protect guests' privacy falls short of their intentions

Previous research reported that privacy is less of a concern for Airbnb hosts when using SHDs, and if they do have concerns, it is about their own privacy instead of guests' (e.g., guests accessing hosts' information through SHDs) [15]. Similarly, Mare et al. [36] did not find guests' privacy as one of hosts' concerns when using SHDs. Our findings suggest quite the opposite: Airbnb hosts consider guests' privacy when they decide where to place smart cameras (Section 4.1), making sure they log out or reset the devices from guests' accounts (Section 4.2.1), monitoring data only when necessary (Section 4.2.3), restraining from controlling the devices when guests are visiting (Section 4.2.2), and making sure to disclose cameras on their properties (Section 4.3.2). All of these behaviors were previously unreported.

However, hosts' effort to protect guests' privacy falls short of their intentions, especially when it comes to managing data (Section 4.2.3). We found that our participants often did not have a clear threat model, which makes them unaware of the privacy implications behind their practices. For example, some of our participants shared accounts with property managers (e.g., housekeepers, cleaners) but did not consider them as potential entities that could infringe on guests' privacy. In addition, real-time monitoring by our participants was common. Granted, our participants tried to monitor their property and guests only when necessary (e.g., through notifications) but also admitted that they felt the urge to check on their property based on their "gut feelings", and did so. Similarly, our participants gave guests limited control and wanted to override their controls if necessary (e.g., temperature settings). Not to mention that hosts do not, if rarely, delete data collected by the devices after guests' visit.

Perhaps the lack of hosts' privacy-protecting measures that we've identified stem from the conflicting need between wanting to protect host's property and wanting to protect guest's privacy. The lack of guidance from platforms on how to use smart devices in a way that protects guests' privacy, and hosts' precarious position as gig-workers [10,14,48], requires constant proof-of-business from either side at the expense of guests' privacy or the security of property. Next, we discuss what we can and should do in terms of providing a clear guideline for hosts and guests to create a safe and privacy-protecting way to use smart devices in rental properties.

5.3 Insufficient guidelines/policies to support hosts

The STR platforms that we investigated in this study are Airbnb and Vrbo, and they each have their own guidelines and policies about the usage of smart devices on their properties.

According to Airbnb's guidelines regarding "use and disclosure of security cameras, recording devices, noise decibel monitors, and smart home devices" monitoring devices (e.g., security cameras, recording devices) are banned indoors but allowed outdoors if hosts disclose in listing's description. Noise decibel monitors (i.e., devices that assess sound level but do not record audio) are allowed indoors and hosts must disclose its presence, but not the location. Hosts are encouraged but not required to disclose SHDs and hosts are encouraged to provide options to guests to disable or unplug them [43]. Vrbo's policies regarding "surveillance devices at property" includes devices that capture image, audio, video, geolocation, personally identifiable information (PII), and internet activity. These devices are not allowed in the property, except for smart devices that cannot be remotely controlled if they are disclosed and given the option to disable them. Security cameras and smart doorbells may be used outside only for security purposes, if their locations are disclosed in multiple channels, access to data is limited, and deletion of data when no longer needed. Noise monitoring devices should be disclosed. These policies are enforced [53].

Although our intention was not to directly compare Airbnb's and Vrbo's guidelines and policies, we found that Vrbo's policies were clearer (e.g., definition) and more comprehensive (e.g., data management). That being said, it is important to note that not all participants were aware of their platforms' policies and guidelines, and this was true even for Vrbo, which had more rigorous policies than Airbnb's. Part of the problem is that some hosts are not aware of the existence of these policies and guidelines, and were not enforced to do so in the case of Airbnb. Even hosts who knew about the guidelines skimmed through it, thought it was irrelevant because they did not have security cameras/recording devices, or skipped disclosing other devices than security cameras/recording devices. The lack of guidance and enforcement to communicate whether hosts have smart devices in their properties is concerning and regrettable, considering how our participants thought these policies and guidelines were positive (e.g., creating a norm around smart device usage in rental properties) and acknowledged that it was a shared effort with involved stakeholders (e.g., matter of public opinion).

Therefore, we suggest and argue that platforms improve their policies and guidelines, not only with their contents, but also in how they address and enforce them with their users (e.g., hosts and guests). Many of the improvements to Airbnb's guidelines can be referred from Vrbo's policies, and we think this is important considering the prevalence and popularity of Airbnb for STRs [49].

Providing guidelines beyond types of devices. Our participants were confused with Airbnb's guidelines for devices other than cameras. For example, our participants were confused about smart speakers because they thought that smart

speakers do not intentionally record people and, therefore, are not recording devices. Airbnb has a more relaxed approach to SHDs; they "encourage" hosts to disclose SHDs and to give guests the option to disable or unplug the devices. Vrbo's definition of surveillance devices (i.e., devices that capture image, audio, video, geolocation, PII, internet activity) practically bans SHDs inside the property. The only exception is when these devices are not remotely controlled, which is difficult to achieve unless the host gives guests complete access/control of the devices. The ambiguity and complexity of platforms' guidelines/policies left our participants confused.

This is especially concerning since previous research found that Airbnb guests were concerned about devices that could potentially monitor them [36, 54], not to mention people's privacy concerns with smart speakers in general [1, 23, 29]. Therefore, we recommend that platforms consider the types of data collected by the devices, rather than the devices themselves when defining monitoring/surveillance devices.

Considering interconnected, multi-functioning devices. All of our participants agreed that smart cameras in bedrooms or bathrooms were unacceptable. However, at the time of the study, Airbnb allowed smart cameras indoors, and we had participants who placed smart cameras in private and shared areas (e.g., living room). Now, Airbnb bans smart cameras indoors. This shows that guidelines and policies regarding smart devices in STRs are evolving and ever-changing. Although Airbnb's recent update in its guidelines is a step towards protecting guests' privacy, there is more to consider. Hosts are still not required to disclose their SHDs, which is concerning when we think about SHDs with multiple functionalities (e.g., smart speakers with embedded cameras, smart TVs with audio/video capabilities). Furthermore, the interconnectivity of SHDs complicates the privacy implications (e.g., data shared among SHDs). As guidelines/policies shape norms in using SHDs in STRs, there is much more room for improvement.

Supporting SHDs' data management practices. Platforms should also provide guidelines/policies on how to manage data collected by SHDs because, ultimately, it is data privacy that matters to people's privacy concerns [51]. Currently, only Vrbo has some instructions for data management (e.g., limiting access to data, unnecessary data deletion), and Airbnb, as a more popular platform, should adopt these instructions in its guidelines. Account sharing and retention periods are other considerations in improving platforms' policies/guidelines. Considering that our participants shared their accounts with guests and property managers (e.g., housekeepers and cleaners), platforms should remind hosts to think about who they are sharing data with when they are sharing accounts. Next, since our participants depended on devices' default data deletion or were reluctant to delete data because they needed proof of business, platforms can suggest hosts delete data after guests' complaint period (e.g., 60 days).

Engaging both hosts and guests on SHDs disclosure. Disclosure is a form of *notice-and-choice*, which is prone to fail due to fatigue or negligence [47]. Thus, platforms should be more active during the disclosure process through better design, encouraging more engagement from hosts and guests.

For hosts, platforms should encourage, if not mandate, the disclosure of hosts' devices throughout their hosting and booking services, instead of just the beginning. Designers can make it mandatory for hosts to disclose their smart devices when registering their homes. The platform should also regularly check in with hosts to update their disclosures, considering hosts might add or remove their devices later. For guests, platforms should display the disclosure information more prominently on the listing, and should actively seek guests' confirmation by displaying such information during the guest's initial inquiry or the final confirmation of booking.

Currently, disclosure of security cameras is buried under irrelevant sections (e.g., the amenity section on Airbnb). When the SHDs in question is not a camera, the device does not even have its own dedicated space to be disclosed. Given that guests often prioritize price and location when booking for STRs, we believe asking for proactive consent from the guests could be more effective than passively showing such information on the listing only.

6 Conclusion

Our study explored the possibility of privacy negotiation between short-term rental (STR) hosts and guests by investigating hosts' practices on usage, management, and disclosure of smart home devices (SHDs), which provides valuable insight into hosts' willingness to accommodate guests' privacy. We conducted online interviews with 15 STR hosts and found that hosts consider guests' privacy when using SHDs: what types of devices they choose to use and locate them, logging out from guests' accounts, limiting monitoring, and disclosing cameras. However, we also found that hosts experience a dilemma between protecting their property versus protecting guests' privacy, therefore, making their efforts fall short of valuing guests' privacy. We identify platforms' insufficient support as the fundamental problem, leaving hosts astray in communicating with guests. We discuss ways to engage both hosts and guests to care about this matter by suggesting improvements to platforms' policies and guidelines, as well as design recommendations for features and functions to support communication.

Acknowledgments

This research is supported by an NSF SaTC CORE program under award number 2232656, and an NSF SaTC Frontiers program (SPLICE) under award number CNS-1955805.

References

[1] Noura Abdi, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. Privacy Norms for Smart Home Personal Assistants. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–14, May 2021.

[2] Amazon. How does drop in work? https://www.amazon.com/gp/help/customer/display.html?nodeId=GS3WRTSRKD2U6MCK.

[3] Amazon.com. Immersive voice experiences. https://developer.amazon.com/en-US/alexa/alexa-for-hospitality.

[4] 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, July 2018.

[5] Natã M. Barbosa, Joon S. Park, Yaxing Yao, and Yang Wang. "What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *Proceedings on Privacy Enhancing Technologies*, 2019(4):211–231, October 2019.

[6] Nicole Bergen and Ronald Labonté. "everything is perfect, and we have no problems": detecting and limiting social desirability bias in qualitative research. *Qualitative health research*, 30(5):783–792, 2020.

[7] 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.

[8] Kelly Caine. Local standards for sample size at chi. In *Proceedings of the 2016 CHI conference on human factors in computing systems*, pages 981–992, 2016.

[9] Dan Calacci, Jeffrey J. Shen, and Alex Pentland. The cop in your neighbor's doorbell: Amazon ring and the spread of participatory mass surveillance. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), nov 2022.

[10] Mingming Cheng and Carmel Foley. Algorithmic management: The case of airbnb. *International Journal of Hospitality Management*, 83:33–36, 2019.

[11] Yushi Cheng, Xiaoyu Ji, Tianyang Lu, and Wenyuan Xu. On detecting hidden wireless cameras: A traffic pattern-based approach. *IEEE Transactions on Mobile Computing*, 19(4):907–921, 2019.

[12] CNET. 9 devices every airbnb host should put in their rental, 2018. https://www.cnet.com/home/smart-home/devices-every-airbnb-host-should-put-in-their-house/.

[13] 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. *Proc. Priv. Enhancing Technol.*, 2021(4):54–75, 2021.

[14] Suzanne C De Janasz, Sowon Kim, Joy Schneer, Nicholas J Beutell, and Carol Wong. Work-family integration and segmentation in the gig economy: Airbnb hosts' challenges and strategies. In *Academy of Management Proceedings*, volume 2020, page 20130. Academy of Management Briarcliff Manor, NY 10510, 2020.

[15] 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*, CHI EA '20, pages 1–8. Association for Computing Machinery, 2020.

[16] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, May 2019.

[17] Rob Gabriele. Vacation surveillance: What travelers think about airbnb security cameras, 2023. https://www.safehome.org/home-security-cameras/traveler-perceptions-airbnb-cameras/.

[18] Radhika Garg and Christopher Moreno. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(2):1–21, June 2019.

[19] 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.

[20] 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.

[21] Yangyang Gu, Jing Chen, Cong Wu, Kun He, Ziming Zhao, and Ruiying Du. Loccams: An efficient and robust approach for detecting and localizing hidden wireless cameras via commodity devices. *Proceedings of the*

ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 7(4):1–24, 2024.

[22] Weijia He, Nathan Reitinger, Atheer Almogbil, Yi-Shyuan Chiang, Timothy J. Pierson, and David Kotz. Contextualizing interpersonal data sharing in smart homes. *Proceedings on Privacy Enhancing Technologies*, 2024(2), 2024.

[23] 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.

[24] Md Nazmul Islam and Sandip Kundu. Preserving iot privacy in sharing economy via smart contract. In *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 296–297. IEEE, 2018.

[25] 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.

[26] 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, April 2022.

[27] Jungsun Kim, Mehmet Erdem, and Boran Kim. Hi alexa, do hotel guests have privacy concerns with you?: A cross-cultural study. *Journal of Hospitality Marketing & Management*, pages 1–24, 2023.

[28] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. "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*, pages 1–14, 2021.

[29] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–31, 2018.

[30] Tu Le, Alan Wang, Yaxing Yao, Yuanyuan Feng, Arsalan Heydarian, Norman Sadeh, and Yuan Tian. Exploring smart commercial building occupants' perceptions and notification preferences of internet of things data collection in the united states. In *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, pages 1030–1046. IEEE, 2023.

[31] Tu Le, Zixin Wang, Danny Yuxing Huang, Yaxing Yao, and Yuan Tian. Towards real-time voice interaction data collection monitoring and ambient light privacy notification for voice-controlled services.

[32] Patricia Leavy. *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. Guilford Publications, 2022.

[33] Anna Lenhart, Sunyup Park, Michael Zimmer, and Jessica Vitak. "You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2):247:1–247:34, October 2023.

[34] Heather Richter Lipford, Madiha Tabassum, Paritosh Bahirat, Yaxing Yao, and Bart P Knijnenburg. Privacy and the internet of things., 2022.

[35] Diba Malekpour Koupaei and Kristen Cetin. Smart thermostats in rental housing units: Perspectives from landlords and tenants. *Journal of Architectural Engineering*, 27(4):04021042, 2021.

[36] 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.

[37] 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*, 2022.

[38] 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, October 2020.

[39] Dana McKay and Charlynn Miller. Standing in the Way of Control: A Call to Action to Prevent Abuse through Better Design of Smart Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, pages 1–14, New York, NY, USA, May 2021. Association for Computing Machinery.

[40] Phoebe Moh, Pubali Datta, Noel Warford, Adam Bates, Nathan Malkin, and Michelle L. Mazurek. Characterizing Everyday Misuse of Smart Home Devices. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2835–2849, May 2023.

[41] Sara Morrison. Google assistant's new guest mode is more private, but there's a trade-off, 2021. https://www.vox.com/recode/22229008/google-assistant-guest-mode.

[42] Savvas Papagiannidis and Dinara Davlembayeva. Bringing smart home technology to peer-to-peer accommodation: Exploring the drivers of intention to stay in smart accommodation. *Information systems frontiers*, 24(4):1189–1208, 2022.

[43] Community policy. Use and disclosure of security cameras, recording devices, noise decibel monitors, and smart home devices. https://www.airbnb.com/help/article/3061.

[44] Johnny Saldaña. *The Coding Manual for Qualitative Researchers*. SAGE, 2nd ed edition, 2013.

[45] Shane Schutte. *Tenant Sentiment Effects of Smart Home Technology in Short-Term Rentals*. PhD thesis, University of Nebraska at Omaha, 2023.

[46] skatun. Smart speakers treated as surveillance. https://airhostsforum.com/t/smart-speakers-treated-as-surveillance/31758.

[47] Robert H Sloan and Richard Warner. Beyond notice and choice: Privacy, norms, and consent. *J. High Tech. L.*, 14:370, 2014.

[48] Robert Sprague. Are airbnb hosts employees misclassified as independent contractors? *U. Louisville L. Rev.*, 59:63, 2020.

[49] Statista. Airbnb - statistics & facts. https://www.statista.com/topics/2273/airbnb/#topicOverview.

[50] Aron Szanto and Neel Mehta. A host of troubles: Re-identifying airbnb hosts using public data. *Technology Science. Oct*, 2018.

[51] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. "I don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*, pages 435–450, 2019.

[52] 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 *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2022.

[53] Vrbo. Vrbo's policy on surveillance devices at a property. https://help.vrbo.com/articles/What-is-HomeAway-s-policy-on-surveillance-devices-at-a-property.

[54] Zixin Wang, Danny Yuxing Huang, and Yaxing Yao. Exploring Tenants' Preferences of Privacy Negotiation in Airbnb. In *Proceedings of the 32nd USENIX Security Symposium*, 2023.

[55] Chris Welch. The wynn las vegas is putting an amazon echo in every hotel room, 2016. https://www.theverge.com/circuitbreaker/2016/12/14/13955878/wynn-las-vegas-amazon-echo-hotel-room-privacy.

[56] Meredydd Williams, Jason R C Nurse, and Sadie Creese. "Privacy is the Boring Bit": User Perceptions and Behaviour in the Internet-of-Things. In *15th International Conference on Privacy, Security and Trust (PST)*, 2017.

[57] New York Times Wirecutter. If you've turned your home into an airbnb, you need smart devices, 2020. https://www.nytimes.com/wirecutter/blog/airbnb-smart-devices/.

[58] Kevin Wu and Brent Lagesse. Do You See What I See? Detecting Hidden Streaming Cameras Through Similarity of Simultaneous Observation. In *2019 IEEE International Conference on Pervasive Computing and Communications*, pages 1–10, March 2019.

[59] 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.

[60] 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.

[61] Eric Zeng, Shrirang Mare, Franziska Roesner, Santa Clara, Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security*, 2017.

[62] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. How usable are ios app privacy labels? *Proceedings on Privacy Enhancing Technologies*, 2022.

[63] Yunxia Zhu, Mingming Cheng, Jie Wang, Laikun Ma, and Ruochen Jiang. The construction of home feeling by airbnb guests in the sharing economy: A semantics

perspective. *Annals of Tourism Research*, 75:308–321, 2019.

[64] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities. *Proceedings on Privacy Enhancing Technologies*, 2024.

A Interview protocol

Hi, thanks for joining us today. I am [name] from [institution] and these are my colleagues. Today, we'd like to talk with you about your experiences using SHDs on your STR property. Before we begin, we kindly request your consent for this study.

To proceed with this process, I will start the recording now, and then we can go ahead with the oral consent. The recordings will only be accessed by us [two or three depending on who are in the meeting].

May I please have your name and today's date? Do you agree to participate in this study? Can you please verify the code that we've sent to your [Airbnb/Vrbo] account?

Thank you for your patience and understanding. We emphasize that you are under no obligation to answer any questions that you are uncomfortable with. You are free to skip any questions and you can withdraw from this study at any time you wish. Do you have any questions before we start? [Take questions] If you have no further questions about the study, let's start.

We are interested about your experiences with using SHDs on your STR property. First, we would like to define what SHDs are: SHDs are household items that are connected to the Internet or a home network to enhance functionality, connectivity, and efficiency within the home. Examples include smart speakers (e.g., Amazon Echo or Google Home), smart lights (e.g., Philips Hue), smart thermostats (Google Nest), and smart locks and security cameras. Please note that we do not include personal devices such as computers, smartphones, tablets, and smartwatches in our definition. Having that in mind, we first wanted to ask about your motivations on using SHDs on your property. [check with survey entry and ask] Can you describe your [Airbnb/Vrbo] property? (e.g., how many, what type, layout) What types of SHDs do you have on your [Airbnb/Vrbo] property? Why did you buy those devices? Where are your SHDs located and what was the reason for locating them there? prompt: How long have you had those SHDs on your [Airbnb/Vrbo] property?

Next, we want to know more about your experience of using SHDs on your STR property. How do you manage your SHDs when your guests visit? (e.g., changing devices' location, turning on/off the devices, reminding guests of their presence, managing accounts and data). Are there any things you do differently to manage your SHDs *before/during/after* guests' visit? Are there any challenges you had using SHDs on your [Airbnb/Vrbo] property with your guests? Any conversations? What did you talk about? prompt: were there any guest comments that mentioned SHDs on your [Airbnb/Vrbo] property?

We're especially interested in how you disclose your devices to your guests. Can you tell us if and how you described your SHDs in your [Airbnb/Vrbo] listings? Are there any considerations you have when disclosing SHDs to your guests? (e.g., types of devices, location of devices) Are there SHDs you absolutely think you need to disclose to your guests? Are there SHDs you don't think you need to disclose to your guests? Why?

Thinking about how to disclose your SHDs to your guests, When would you like to do it, and how? (e.g., through the listing, when guests are booking, reminding guests through manual)

So, Airbnb allows the use of cameras and recording devices if they are disclosed in the public and common spaces. Airbnb does not allow if devices are not disclosed and/or are in public spaces. [show Airbnb guidelines; make sure to zoom in when sharing screen; can also share link in chat; make sure to give enough time for participants to read] [2] How familiar are you with the guidelines? How did you know about it? What do you think about the guideline? (e.g., understandable? useful?)

We're also curious about your concerns when using SHDes on your [Airbnb/Vrbo] property. What do you think are the benefits of having SHDs on your [Airbnb/Vrbo] property? What do you think are the drawbacks of having SHDs on your [Airbnb/Vrbo] property? Can you think of any potential issues that might arise from using SHDs on your [Airbnb/Vrbo] property? What are the issues that you might face as a host? What are the issues that guests might face?

[If participant does not mention any privacy issues] Here are some privacy issues that might arise from using SHDs in a STR property. For example, there was a debate among Airbnb hosts about a guest complaining that they were uncomfortable with smart speakers and whether hosts should disclose and/or use them [46]. Have you experienced any of these issues? What happened? How did you resolve these issues? If not, do you think any of these issues might happen to you? What would you do?

Thinking of the people involved in resolving these issues, (If that happened) What did your guests do? (If not) What might you want guests to do to resolve those conflicts? What might you want [Airbnb/Vrbo] to do to resolve those conflicts? What do you think might help to prevent these issues?

[check if team members have any remaining questions left] Thank you for your time today, before we end, we would like to ask if there was anything you wanted to say but didn't get to, or if you had any questions for us.

[2] We introduced Vrbo's policies for participants who hosted on Vrbo

B Final codes, sub-codes, and their descriptions

Codes and sub-codes	Descriptions
STR property description	*Participants' description of their STRs regarding...*
Size	how big the property is in terms of the types of property hosted (e.g., entire house, private room) and the types of rooms hosted (e.g., 2 bed 2 bath).
Residence	the objectives of residence of the property hosted (e.g., primary, secondary, investment).
Characteristics	how the property is marketed to the guests (e.g., farmhouse) often shaped by local events and seasonality (e.g., ski-event, metro-area).
Guest characteristics	the types and sizes of guests (e.g., business, family).
Types and location of SHDs	*Participants mentioning what kind of devices they use and where.*
Motivations for using smart home devices	*Participants' description of why they use SHDs (similar to Advantages but different in that these are tied to intentions and expectations).*
Home automation	To automate their home.
Guest experience	To improve guests' experience (e.g., providing a seamless experience).
Monitoring property	To monitor the house.
Monitoring guests	To monitor guests (e.g., to check the number of guests).
Safety and security	For safety and security reasons both for the property and guests (e.g., fire, flooding).
Energy conservation	To save energy (e.g., temperature, lights).
Remote control	To have control of their property from remote.
Interconnectivity	To connect with other devices in the house.
Motivations for NOT using smart home devices	*Any reasons for participants' reluctance to using SHDs due to (similar to Disadvantages but different in that these are more tied to intentions and expectations)...*
Guests' privacy	Concerns about guests' privacy.
Cost	Concerns about cost.
Theft	Concerns about theft.
Technical difficulties	Concerns about the technical difficulties involved in using SHDs (e.g., installation).
Mindfulness	Wanting to provide guests with time away from technology.
No need	Participants' disinterest in using (specific) smart home devices.
Advantages of using smart home devices	*Participants' comment on the advantages of using smart home devices on their rental property (similar to Motivations but different in that these are lived experiences).*
Conserve energy	Using smart home devices saves energy consumption.
Safety and security	Using smart home devices provide safety and security to the property and guests.
Proof of business	Using smart home devices provide hosts with proof of business when they need evidence.
Entertainment	Using smart home devices provide entertainment for guests (e.g., smart TVs).
Visibility	Using smart home devices provide visibility (e.g., guests' activity, smart home data) to hosts.
Guest experience	Using smart home devices provide a better experience for guests (e.g., seamless entry).
Remote control	Using smart home devices provides the convenience of remotely controlling the property.

Codes and sub-codes	Descriptions
Disadvantages of using smart home devices	*Participants' experiences of challenges in using smart home devices on their rental property (similar to Motivations for NOT using SHDs but different in that these are more lived experiences).*
Technical failures (internal)	Facing technical failures due to device defects such as loss of network connection and/or battery outage.
Technical difficulties	Facing technical difficulties due to one's lack of technical proficiency, such as smart home devices being too complicated to manage.
(Potential) Theft	Guests stealing stuff from home, especially smart home devices.
Guest confusion	Guests being confused on how to use smart home devices on rental property.
Invasion of guests' privacy	Using smart home devices invades guests' privacy.
Guest misuse	Guests using smart home devices in a way that is not intended by the host (e.g., purchase of items)
Lack of guest control	Participants not being able to provide enough control for guests.
Reasons for device purchase and usage	*Reasons that participants buy certain devices and use it in a certain way.*
External sources	Participants learn and/or hear from external sources (e.g., other Airbnb hosts, online forums).
Integration	Choosing a specific brand/company to integrate the devices.
Brand reputation and trust	Preference based on reputation and trust to a specific brand/company.
Smart home device management	*Participants' management of the smart home devices and data.*
Accounts and passwords	Whose accounts are being used and how passwords are shared for the smart home devices.
Shortcuts	Creating workarounds to manage their smart home devices (e.g., using text shortcuts to remotely manage devices).
Access control	Access control mechanisms for guests using smart home devices (e.g., manual control, smartphone apps).
Notifications	Setting up notifications to manage SHDs.
Disclosure	Participants consideration of disclosure as a part of their management.
Routines and/or schedules	Participants set routines and schedules to manage their devices
Manual management	Physically managing the devices
Reviewing and deleting data	Reviewing and deleting data collected by SHDs at any time of the guests' stay.
Upgrade	Upgrading soft/hardware for SHDs
Disclosing smart home devices	*Participants' perception of whether or not to disclose any/certain SHDs to guests.*
Must	Smart home devices that participants think they absolutely should disclose to their guests.
Unsure	Smart home devices that participants are unsure if they should disclose to their guests.
Not disclose	Smart home devices that participants do not disclose to their guests for any reason.
Methods of disclosure	*How participants disclose/communicate their SHDs to guests (similar to Disclosure considerations but different in that these are actual practices).*
Property listing	Participants disclosing their SHDs in the property listings.
Property description	Participants disclosing their SHDs in the property descriptions.
Messaging	Participants disclosing their smart home devices through messaging (e.g., platform, external chats) with the guests.
Additional instructions	Participants disclosing their smart home devices with additional instructions (e.g., physical manual)
Preference for disclosure methods	*Participants' preference in how to disclose their SHDs.*

Codes and sub-codes	Descriptions
Disclosure considerations	*The kinds of considerations participants put into when they are thinking of disclosing SHDs to guests (similar to Methods of disclosure but different in a way that it might not be practiced).*
Instruction for guests	Leaving additional instructions for guests.
Respect to guest privacy	Thinking about how to respect guests' privacy when disclosing SHDs
Accounts	Disclosing who's account is associated with the device.
Data visibility	If participants consider disclosing what data is visible to whom.
Familiarity with STR policies/guidelines regarding SHDs	*Participants' self-reported familiarity with platforms' policies/guidelines regarding smart devices.*
Perceptions of platforms' policies/guidelines	*Participants' perceptions of platforms' policies/guidelines.*
Positive	Any positive reactions to platforms' policies/guidelines regarding smart devices.
Negative	Any negative reactions to platforms' policies/guidelines regarding smart devices.
Neutral	Any neutral reactions to platforms' policies/guidelines regarding smart devices.
Perception of surveillance/monotoring	*Participants' perceptions of surveillance versus monitoring.*
Needs/wants in platforms' policies/guidelines	*Participants' wants and needs regarding platforms' policies/guidelines regarding smart devices.*
Willingness to negotiate/accommodate	*Participants' willingness to negotiate, accommodate, and compromise with guests about their usage of SHDs to meditate guests' concerns.*
Non-negotiables	*Participants' reluctance to negotiate and reasons why.*
(Potential) conflicts with guests	*(Potential) conflicts with guests regarding the usage of SHDs in rental property.*
Resolving conflicts	*How participants resolve, or plan to resolve conflicts with guests regarding the usage of SHDs in rental property.*
Expectations towards guests	Participants' expectations of guests when they are in conflict.
Communication	Participants' mentioning of communication as a strategy to resolve conflicts with guests around the usage of SHDs.
Expectations towards platforms	Participants' expectations of platforms when they are in conflict with guests (e.g., moderation)
Transparency	An emphasis on being transparent about the usage of SHDs to guests when resolving conflicts.
Empathy	An emphasis on being empathetic to guests when resolving conflicts (e.g., If I were a guest...).
Explanation	An emphasis on explaining to guests the details of using SHDs with guests (e.g., why, where, how).
Granting access	Participants granting access to guests to resolve conflicts around SHDs.
Unreasonable requests from guests	*When participants think guests' requests are unreasonable, therefore no need to accommodate.*
Other stakeholders	*People involved in managing the rental property beside the hosts (e.g., caretakers, neighbors, cleaners, and property managers).*
Unsure	*Quotes that are interesting but unsure where they fit.*
Good quotes	*Quotes that represent, highlight codes and themes; Make sure that ends up in the writing.*
Tech-savvy host	*Participants who have indications that they are tech-savvy (e.g., background in IT).*

Codes and sub-codes	Descriptions
SHDs in the background	*Participants' strategies to deploy SHDs in a way that delivers guests with a seamless experience.*
Smart home adoption	*How participants adopt SHDs to their STRs (e.g., gradual).*
Needs/wants in SHD functionality	*Participants' needs/wants in SHD functionality to ease the use in their STRs (e.g., guest mode).*
Negotiation practices	*Any negotiation practices employed by participants to resolve conflicts with guests.*
Interesting but irrelevant	*Quotes that are interesting and potentially relevant to answering our RQs.*