Proceedings on Privacy Enhancing Technologies ; 2020 (2):436–458

Shrirang Mare*, Franziska Roesner, and Tadayoshi Kohno

Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts

Abstract: Consumer smart home devices are becoming increasingly pervasive. As Airbnb hosts deploy smart devices in spaces shared with guests, we seek to understand the security and privacy implications of these devices for both hosts and guests. We conducted a large-scale survey of 82 hosts and 554 guests to explore their current technology practices, their preferences for smart devices and data collection/sharing, and their privacy and security concerns in the context of Airbnbs. We found that guests preferred smart devices, even viewed them as a luxury, but some guests were concerned that smart devices enable excessive monitoring and control, which could lead to repercussions from hosts (e.g., locked thermostat). On average, the views of guests and hosts on data collection in Airbnb were aligned, but for the data types where differences occur, serious privacy violations might happen. For example, 90% of our guest participants did not want to share their Internet history with hosts, but one in five hosts wanted access to that information. Overall, our findings surface tensions between hosts and guests around the use of smart devices and in-home data collection. We synthesize recommendations to address the surfaced tensions and identify broader research challenges.

Keywords: Airbnb, Privacy, Security, Smart devices, Smart Homes

DOI 10.2478/popets-2020-0035
Received 2019-08-31; revised 2019-12-15; accepted 2019-12-16.

1 Introduction

Smart devices and smart home platforms, increasingly pervasive, have already raised a number of privacy and security concerns for those who use them [13, 21, 24, 27, 38, 41, 43, 44]. In this work, we study the use of—and privacy and security concerns with—smart devices not in people's *own* homes, but in the homes they rent temporarily, specifically via home sharing platforms like Airbnb [18]. We focus in particular on the dynamics between two stakeholder groups: hosts (who choose which smart devices to install in their homes) and guests (who temporarily reside in these homes).

Airbnbs and other short-term rentals represent a growing use case for smart devices. Smart devices enable hosts to remotely manage their Airbnb and may offer convenience to guests. But, at the same time, smart devices raise security and privacy concerns for both hosts and guests. Currently, it is unclear how and what smart devices are being used in Airbnbs, and how hosts and guests think about them. It is important to understand this so we can inform both how hosts should set up smart devices in Airbnb, and how we (researchers and designers) might design smart home devices with the Airbnb use case in mind. In this work, we study the unexplored space—smart devices in short-term rentals—to raise issues and provide recommendations for future research. Specifically, we explore the following research questions:

RQ1 What smart devices do *guests* want in Airbnbs, what data they do not want to share with hosts, and what are their security and privacy concerns related to smart devices in Airbnb?

RQ2 What smart devices do *hosts* want in their Airbnb, what data they want to monitor in their Airbnb, and what are their security and privacy concerns related to smart devices in their Airbnb?

RQ3 Considering the views of guests and hosts, where do their views match and conflict?

Informed by the vast literature on smart device privacy and security, as well as known risks and vulnerabilities with smart devices, we conducted a survey of 82 hosts and 554 guests on Amazon MTurk. We asked them their preferences for smart devices, for in-home data collection/sharing, and risk perceptions for different scenarios that could occur in Airbnbs. The survey also included several open-ended questions for them to explain their preferences and share past experiences.

We found that guests were largely neutral or preferred smart devices in Airbnbs, but that their prefer-

***Corresponding Author: Shrirang Mare:** University of Washington and Indiana University
Franziska Roesner: University of Washington
Tadayoshi Kohno: University of Washington

ences were highly contextual (e.g., depending on Airbnb location, travel purpose). Many guests did not want smart cameras, voice assistants, or motion sensors due to privacy concerns, and some guests did not want smart thermostats for fear that hosts may lock the thermostat setting. At the same time, hosts reported having smart devices in their Airbnbs and wanting data from devices that can help them identify guests who break house rules.

Comparing guests and hosts, we found that both expressed similar preferences overall in terms of which devices to have in an Airbnb, but their preferences differed on where those devices should be placed, how they should be used, and what data should be collected. When reporting their *own* device preferences, both guests and hosts acknowledged the needs of and risks to the *other*. For example, guests expressed concern over privacy or lack of control (e.g., locked thermostat), but also acknowledged hosts' need for smart devices to monitor their property; and hosts expressed concern for guests' privacy but also reported a need for smart devices. These findings suggest that there is a need for smart devices in Airbnbs, but the design space is nuanced, and meeting the different expectations of both hosts and guests will be challenging.

Informed by our findings, we take a step back to ask: How should smart devices be designed in consideration of the functionality, privacy, and security needs of *both* hosts and guests? To tackle this problem, we use our findings to synthesize concrete design recommendations and to identify directions for future research. For example, we suggest ways to apply the principle of least-privilege to meet hosts' needs without unduly violating guests' privacy, guidelines for responsible device disclosure, and ways to reduce access control burden for hosts and guests.

In summary, our contributions include:

1. The first in-depth exploration of smart devices in shared homes (homes shared temporarily via platforms like Airbnb) with stakeholder groups comprised of hosts and guests.
2. A large-scale study of Airbnb hosts and guests to understand—from a privacy and security perspective—their views, behaviors, and concerns about smart devices in Airbnbs (Section 5).
3. Concrete design recommendations to address key privacy and security tensions (between guests and hosts) that surfaced in our research (Section 6). We also discuss opportunities for future research.

2 Background and related work

We use the term *smart devices* to refer to devices with computation and communication abilities in the context of a home. Smart devices could be used for entertainment (e.g., smart TVs), automation (e.g., motion sensors), sensing (e.g., smart smoke sensors), and/or controlling other devices (e.g., smart thermostats).

We use the term *shared homes* for homes that are rented or shared via home sharing platforms like Airbnb [18], HomeStay [20], and HomeExchange [19]. On these platforms, *hosts* provide homes for temporary stays, and *guests* temporarily stay in those homes.

Different types of home sharing occur on Airbnb. This study focuses on hosts who provide guests with: private access to the entire home (we refer them as *home hosts*); private access to a room in the house (we refer them as *private-room hosts*), and shared access (with host or other guests) to a room in the house (we refer them as *shared-room hosts*).

Airbnb. Prior studies about Airbnb, or home sharing ecosystems in general, largely focused on the financial (e.g., [23]) or social (e.g., [7]) issues. More recently, using reviews that users post on Airbnb, researchers have explored self-disclosure and perceived trustworthiness [26], compared effects of ratings and reviews on user reputation [34], and measured effectiveness of the reviews themselves [8, 15].

From a privacy perspective, researchers have studied the risk of re-identifying hosts using their Airbnb profiles [39], and more recently solutions for detecting hidden cameras in Airbnbs [9, 42]. Our study investigates guests' concerns about hidden cameras, along with several other concerns.

Smart devices in homes. An increasing body of research tackles privacy and security of smart devices, both from the system perspective (e.g., [4, 14]) and from the end-user perspectives (e.g., [24, 43, 44]). Our work contributes to the latter by identifying users' privacy concerns, preferences, and behaviors in a previously unexplored context—Airbnbs.

Prior research on smart home users largely focused on the primary user (the person who set up the smart home). However, researchers are now beginning to explore perspectives of other users, such as secondary users and guests [16, 24, 43]. Zhen et al. studied mental models of smart home users and discovered that primary users would occasionally restrict other users' control to certain devices [43]. Geeng et al. [16] studied interac-

tions between occupants of multi-user smart homes and found varying degrees of cooperation between primary and secondary users, but overall primary users had more control on the smart home devices. In Airbnbs, currently there is no cooperation between hosts (primary users) and guests (secondary users or non-users) during device set up or use. So the power asymmetry between hosts and guests is even greater in Airbnbs; we found supporting anecdotal evidence. Although the *guest* use case exists in both Airbnbs and residential homes (not rentals), the differences in the level of cooperation and trust between a guest and an Airbnb host vs. a home resident may require different considerations when designing for Airbnb guest vs. home guest. A careful analysis of these differences and similarities merits investigation in future research.

Researchers have also conducted survey studies to investigate user opinions about IoT privacy. Martin and Nissebaum surveyed 569 individuals and found that they cared more about the intended use of the data than the sensitivity of the data itself [28]. Emami-Naeini et al. investigated privacy expectations in IoT device use cases and found that privacy preferences were heavily context-dependent [32]. Choe et al. found that American users were especially concerned about connected devices recording and sharing private in-home activities [10].

Our research contrasts with prior work in three ways: (1) we investigate users' preferences for devices in the context of a home shared via Airbnb, (2) we survey both primary users (hosts) and secondary users (guests) of smart home, and (3) we focus on the security and privacy tensions between hosts and guests.

3 Methodology

We first discuss the survey design (Section 3.1) and then present the survey protocol (Section 3.2), data analysis (Section 3.3), recruitment process (Section 3.4), and study limitations (Section 3.5).

3.1 Survey design

We created the survey using an iterative design process. We first created survey questions to address our research goals. We then conducted a 50-participant pre-survey on MTurk to collect free responses to our survey questions. These responses informed our selection of answer choices to multiple-choice questions, and to our list of smart devices, list of information types, and risk incidents that we used in the final survey (Tables 1-3 show these lists). Finally, we tested the survey for understandability with fifteen individuals: ten took the survey online and gave feedback within the survey (using a free-response option with each question); five took the survey during a think-aloud interview. We revised phrasing and UI to resolve any confusion raised during the testing.

We created a Javascript-based Web survey to make our survey interactive (e.g., drag and drop house layout questions; Section 3.2) and to have more conditional control over the survey than is currently possible with survey platform like Qualtrics.

To reduce common biases in the survey, we followed the recommendations on survey design [2, 17, 25, 35]. For example, we did not advertise it as a privacy survey; we chose to ask explicit questions about privacy and security concerns toward the end of the survey, giving participants the opportunity to raise concerns without being primed; we randomized answer choices; and we carefully chose question order and phrasing.

Our goal was to provide an initial exploration of smart devices in Airbnb and to raise issues for future research. We chose to explore a broad range of topics rather than a comprehensive analysis of one topic. And to do so while keeping the cognitive burden of the survey reasonable, we had to limit the depth of questions. Next, we discuss our rationale for the tradeoffs we made in designing the survey.

Questions about smart devices. The term "smart" can mean different things to different people, and people have different levels of understanding about the features and capabilities of smart devices. To avoid misinterpretation participants need information, which if too detailed can overwhelm them and/or bias their responses. We wanted to understand people's preferences about smart devices based on their *current* understanding of smart devices—that is, their natural response, without first being educated. Learning people's natural responses is important because people often make decisions based on their existing mental models. Guests, for example, may encounter smart devices in Airbnb and they may not know all the capabilities of the devices. Therefore, we chose not to provide details about device capabilities, but to provide a definition of smart devices and clear descriptive device names with representative examples.

We defined smart devices as "Internet-enabled devices; these devices usually have built-in Bluetooth or Wi-Fi and can be controlled via a smartphone or a voice assistant (e.g., Amazon Echo)." This definition was pre-

Table 1. List of devices.

Devices
Digital Door Lock (e.g., lock with a keypad)
Door/Window Sensor
Gaming Console (e.g., Xbox, PlayStation)
Motion Sensor
Smart Camera (e.g., Nest camera)
Smart Light (e.g., Philips Hue lights)
Smart Power Outlet
Smart Security System (e.g., ADT)
Smart Smoke Sensor (e.g., NEST smoke sensor)
Smart Thermostat (e.g., Nest thermostat)
Smart TV (e.g., TV with Wi-Fi)
Voice Assistant (e.g., Amazon Echo)

Table 2. List of data types.

Data types
If doors/windows are left unlocked
If there is a water leak in the house
Internet history (e.g., sites visited)
Noise level in the house
Number of guests staying
Smoking activity
Thermostat setting
TV watch history
Utility usage (e.g., electricity)
When guests arrive and leave
Visitor activity

Table 3. List of incidents

For host participants
G(uest) breaking house rules
G changing password on devices (e.g., router)
G downloading illegal content on Internet
G installing a secret camera or a microphone
G leaving door/windows unlocked
G misusing resources (or using excessively)
G posting house photos on social media
G sharing passwords with others
For guest participants
A hidden audio recording device
A hidden camera
H(ost) monitors visitor activity
H monitors resource usage (e.g., electricity)
H monitors Internet activity (e.g., sites visited)
Guests are not allowed to control thermostat

sented along with the survey question about smart devices. We used common and descriptive device names (e.g., door/window sensor) so that participants unfamiliar with the devices could make educated guess about the device. For popular smart devices, we included a representative product example (e.g., Amazon Echo with voice assistants) because some people associate a smart device with a product instead of its category name. Finally, for devices such as smart TVs and digital door-locks with no popular representative product, we used a brief description about the device or its basic capability (e.g., TV with Wi-Fi). Table 1 shows devices as shown in the survey.

Questions about data collection/sharing. We were interested in understanding participants' reactions and their sensitivity to the types of data that can be collected in an Airbnb. We showed participants a list of data types (Table 2) and asked hosts to choose what they want to collect and asked guests what they *do not* want to share with hosts. We carefully chose short descriptive labels for the data types, and tested their understandability in our survey testing. Because we wanted to understand participants' reactions based on their own understanding of devices, we chose not to specify any additional details about data collection such as how data was collected, when it was collected, and granularity level. These additional details about data collection can influence people's data sharing preference [28], and we believe they should be investigate in future research.

Questions about risk perceptions. We were interested in understanding participants' perceptions of risk for incidents that could occur in Airbnbs. We identified incidents (listed in Table 3) based on our pre-survey and our review of Airbnb forums. For each incident, we asked participants the likelihood of its occurrence. Because hosts primarily interact with the Airbnb ecosystem through their own Airbnb, we asked hosts the likelihood of the scenario happening in *their* Airbnb. Guests, on the other hand, can encounter any Airbnb when planning their stay, so we asked them the likelihood of the scenario occurring in *any* Airbnb. We also asked participants to rate how upset they would be if an incident happened to them.

3.2 Protocol: Main survey

We used a screening survey to identify guests and hosts, and then conducted separate surveys for them.

Screening survey. The screening survey posed three multiple-choice questions (available in Appendix A.1). First, we asked them which online services do they use (choices included Airbnb). Second, we asked them which home rental services they have used (choices included Airbnb). If participants chose Airbnb in both questions, we asked them the third question: Are you an Airbnb host or guest (or both)? A participant was eligible for our study if they chose Airbnb in the first two questions and answered the third question.

To reduce participation bias, we did not ask directly whether they were an Airbnb guest/host, nor did we disclose our selection criteria. The screening survey was advertised as "a short eligibility survey for a longer task." Initially we excluded individuals who chose all options

in the first question, assuming they were trying to game the screening survey. After we realized that some of these individuals could be eligible participants, we conducted a second round of our survey to include such previously excluded participants in our sample.

Guest survey. The survey had five themes: demographic and general Airbnb usage, current technology practices, smart device preferences, data collection preferences, and risk perceptions. (The full survey is available in Appendix A.2.)

Current technology practices: We showed participants a list of smart devices (Table 1) and asked them which of the devices they *noticed* in any of their past Airbnb stays. We also asked guests the types of passwords they received from hosts (and how), and how they communicated with hosts (e.g., email, Airbnb message).

Device preferences: We asked participants to choose smart devices (Table 1) that they would want in their next Airbnb. For each device, guests could choose one of four options: *Yes*, *Neutral*, *No*, and *Depends (on device location in the house)*. Guests who chose *Yes*, *No*, or *Depends* for any device where asked a follow-up question. For *Yes* and *No* choices, guests were asked to explain their choices in an open-ended response. For the *Depends* choice, guests were shown a house layout and were asked to drag the devices they chose as *Depends* to places they would *not* want them. To make it clear that they have to drag devices to places they would *not* want that device, the devices were shown with prefix "NO" (e.g., "NO-smart camera") and red background; Appendix A.4 shows a screenshot of this question.

Data sharing preferences: We showed guests eleven data types (Table 2) and asked which data they would *not want* to share with their host. We then asked them to explain their choices in an open-ended response.

Risk perceptions: We presented a list of incidents that could occur in an Airbnb (Table 3) and asked participants to rate on a 5-point scale ("extremely unlikely" to "extremely likely") how likely they thought it was that the incident would occur in Airbnbs. We then showed them the same scenarios and asked them to rate on a 5-point scale ("not upset" to "extremely upset") how upset they would be if that incident happened to them. We also gave participants an open-ended question to report any bad experiences or concerns.

Host survey. The host survey had the same five themes as the guest survey with similar questions. We describe here only the questions in the host survey that differed; Appendix A.3 shows the full host survey.

Current practices: We asked hosts the type of their Airbnb, its layout (types of rooms, number of rooms), and the devices they currently have (they were shown the device list but could also report a device not on the list). We then showed hosts a house layout and asked them to indicate where they had set up each of their device by dragging it onto the layout. The layout was generated for each participant based on their Airbnb layout they shared in an earlier question.

Data collection preferences: We asked hosts what data they would like to monitor in their Airbnb; they were shown a list of data types (Table 2) but could also report a data type not on the list. We asked them to explain their choice in an open-ended response.

Risk perceptions: We asked hosts the same two risk perceptions questions that we asked to guests, but we chose different (host-specific) risk incidents (Table 3).

3.3 Data analysis

We used standard approaches to remove clearly low-quality data: we discarded participant data if survey completion time was too short or too long, if any open-ended response was nonsense, and if answers for all the conditions in a Likert-scale question were the same (e.g., all neutral, all disagree). In total, we discarded about 12% of survey data. For the qualitative data (open-ended responses), we used inductive thematic analysis [5] to identify the main themes. For each participant, we created a record of all the open- and close-ended responses; the close-ended responses provided the context to better interpret participants' open-ended explanations. Three researchers reviewed a subset of responses and together iterated on the codes and themes to create a codebook; one researcher used the codebook to code all open-ended responses.

3.4 Ethics and recruitment

We recruited participants on Amazon Mechanical Turk between November 2018 and February 2019, with a second round of survey conducted in August 2019. To reduce selection bias, we did not advertise the study about security or privacy, but as a study about "technology use in Airbnb." All survey questions (except for a few conditional ones) were optional, and participants could skip questions they did not want to answer, without any penalty. The study protocol was approved by our university's human subjects review board (IRB). Participants

received USD 1.5 for completing the survey, which took on average 8 minutes.

3.5 Limitations

This study has some limitations that should be considered when interpreting its findings.

1. Although our sample was comparable to U.S. Airbnb users for age and gender, the survey findings may not generalize to the broader Airbnb population, especially outside the United States.
2. We did not consider multi-function smart devices (e.g., a smart doorlock with a built-in camera), which may have different privacy implications than multiple single-function smart devices.
3. We studied participant preferences based on their current understanding of smart device capabilities. It is likely that different participants may have different understanding about each smart device, which implies, for example, two participants may want a device but for different reasons.
4. For the design choices we made (discussed in Section 3.1) there is a possibility that participants may have misinterpreted some terms and questions; the likely candidates include the smart device "Smart Security System," the data types "Noise level in the house" and "Internet history," and the question on data sharing preferences in the guest survey.
5. The second round of the study was conducted about six months after the first round (discussed in Section 3.2); we compare the two rounds below. The additional time (e.g., news/events about Airbnb or smart devices during this time) may have influenced participant responses in the second round in a way that we have not accounted for.

To compare the two rounds, we compared guest-participant responses to questions on device preferences and risk perceptions. In total, we compared responses to 24 Likert-scale questions: twelve device preferences, six risk incident likelihood ratings, and six risk upset ratings. For each question, we used the Mann-Whitney U test to check whether the median of the responses in one round is significantly higher than the other round; if it is, it would mean that participants in one round rated higher on the Likert-scale than those in the other round. We chose the Mann-Whitney U test because the data is ordinal, and we did not want to make assumptions about the distribution of the data. When reporting test statistics, we report rank-biserial correction (r) [12] as a measure of the effect size; r can range from -1 to 1, with zero indicating no effect. Out of the 24 comparisons, we found significant differences ($p < 0.05$ two-tailed), but with a small-medium effect ($r < 0.3$), in five questions: device preferences for motion sensors ($U = 7609$, $p = 0.01$, $r = 0.22$), smart doorlock ($U = 8213$, $p = 0.04$, $r = 0.16$), security system ($U = 7583$, $p = 0.01$, $r = 0.22$), smart thermostat ($U = 7741$, $p = 0.01$, $r = 0.20$); likelihood rating for incident "Host monitors resource usage" ($U = 7624$, $p = 0.01$, $r = 0.22$); and upset rating for incident "Host monitors Internet activity" ($U = 7627$, $p = 0.01$, $r = 0.22$). These differences may be due to sampling error, demographics differences, or the time between the rounds. Our focus was not to study the changes in participants' preferences over time, so we present the findings (Section 5) from the combined sample.

Despite these limitations, our exploratory study surfaces important insights and observations about people's preferences for smart devices and data collection in Airbnb-like context, and raises future research opportunities.

4 Participants

We conducted the screening survey with 3,000 individuals (in six waves of 500 each). Out of those, 1,477 qualified and received notification about the main survey. A total of 636 participants (82 hosts and 554 guests) took the main survey; 590 participants took the survey in the first round and 46 in the second round. Table 4 summarizes participant demographic. Our sample was roughly gender balanced: 311 participants identified as male (48.9%) and 318 as female (50%). Most participants were young adults (25-44 year range) with a college degree or a graduate/professional degree.

Among our host participants, 36 (43.9%) rented their entire home, 40 (48.8%) rented a private room in their home, and the remaining 6 (7.3%) rented a shared room in their home. Guest participants reported staying in different types of Airbnb. 386 (69.6%) had stayed in an entire home; 239 (43.1%) in a private room; and 35 (6.3%) in a shared room. Guests reported that they used Airbnb to save money (n=414; 74.7%), to get local experience (n=278; 50.2%), or to accommodate large parties (n=127; 22.9%).

Overall, participant demographics was comparable to the demographics of Airbnb users in terms of gender and age [29], and reasons for using Airbnb [7, 30, 31].

Table 4. Demographics of participants.

	Hosts (n=82)	(%)	Guests (n=554)	(%)
Male	40	48.8	271	48.9
Female	40	48.8	278	50.2
Other	2	2.4	5	0.9
Age 18-24	10	12.2	67	12.1
Age 25-34	51	62.2	248	44.8
Age 35-44	15	18.3	139	25.1
Age 45-54	2	2.4	74	13.4
Age 55+	4	4.9	26	4.7
High School	7	8.5	68	12.3
College	44	53.7	301	54.3
Graduate School	23	28.0	141	25.5
Professional School	8	9.8	36	6.5
United States	74	90.2	512	92.4
Other	8	9.8	42	7.6

5 Findings

We first present the results from the guest survey (Section 5.1; RQ1), followed by the results from the host survey (Section 5.2; RQ2), and finally we compare guest and host views from the two surveys (Section 5.3; RQ3).

5.1 Guest findings

We first present the smart devices that guests observed in their past Airbnb stays, and then guests' smart device preferences, their smart device needs, and finally, guests' concerns about smart devices.

5.1.1 Smart devices observed in Airbnbs

What smart devices are currently being used in Airbnbs? To investigate this question, we showed participants a list of twelve smart devices (Table 1) and asked them which devices they previously noticed in Airbnbs. Guests reported the presence of all twelve smart devices, but to varying degrees. The most reported smart devices in Airbnbs were smart TVs (69%), smart door-locks (51%), gaming consoles (37%), smart thermostat (28.8%), and voice assistants (18.4%); other smart devices were reported by 12-15% guests. Guests reported two devices not on our list: Roku and a smart garage opener.

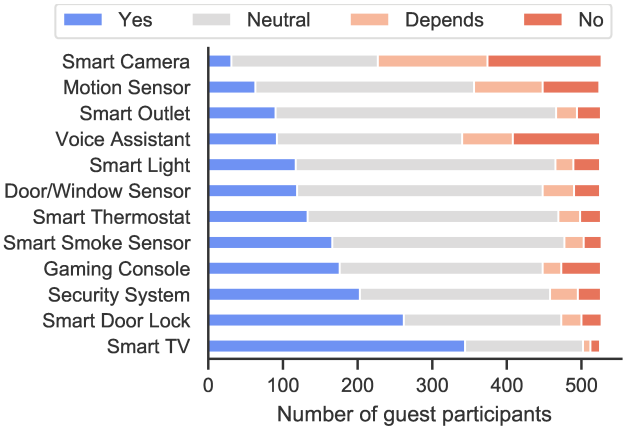

Fig. 1. Guests preferences for smart devices in Airbnbs.

5.1.2 Guests' smart device preferences

On average, of the twelve smart devices that we asked about, guest participants reported a strong preference (chose *Yes*) for three smart devices (mean=3, SD=2.6), a neutral preference for six (mean=5.48, SD=3.49), chose *Depends* for one (mean=0.91, SD=1.45), and chose *No* (do not want device in an Airbnb) for one (mean=1, SD=1.99). The top four devices that participants wanted in Airbnbs were smart TVs, smart door-locks, security systems, and gaming consoles; and the top three devices they did not want were smart cameras, motion sensors, and voice assistants. Figure 1 shows the distribution of guests' preferences for smart devices.

A key point to note is that for every device, some participants wanted it in their Airbnb and some did not. To meet the needs of guests who want specific devices while respecting the concerns of those who do not, we need to understand the underlying factors that could influence guests' preferences.

Factor: Device location. When reporting smart device preferences, guests who chose *Depends* for a smart device were asked in which areas of the house they would *not* want that smart device. The left heatmap in Figure 2 shows areas and number of guests who did not want particular smart devices in those areas. (The center and right heatmaps show where hosts reported setting up smart devices in their Airbnb, which we discuss in Section 5.2.)

Overall, guests did not want smart devices in their bedroom or bathroom, but their preferences varied for exterior areas (e.g., front yard) and areas in the house that could be shared with others (e.g., living room, kitchen). For example, of the 129 guests who chose *Depends* for smart cameras, 122 guests (94.5%)

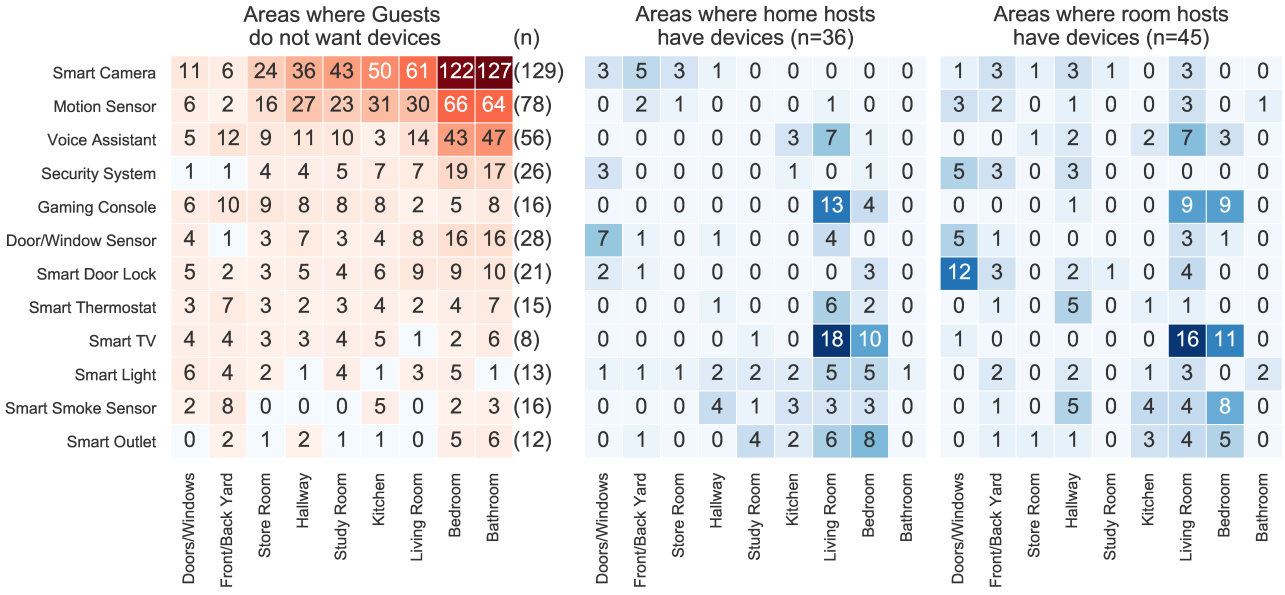

Fig. 2. Smart device preference by location in the house. The left heatmap shows the number of guests who did *not* want smart devices (row) in certain areas (column) in Airbnb; in parenthesis is the number of participants who chose *Depends* for the device in the row. The other two heatmaps (discussed in Section 5.2) show where hosts had set up smart devices in their Airbnbs. All plots share the y-axis.

did not want a smart camera in bedroom, but only 61 guests (47%) said they did not want one in the living room, and even fewer participants were concerned about cameras in other shared spaces.

> I am wary of cameras in the bedroom and bathroom areas. Other areas I am more ok with but not if it's excessive monitoring with cameras on every corner. (G58)

Note that a majority of guests wanted smart doorlocks and security systems (Figure 1) because of the convenience and a sense of safety that these devices offer, but some guests did *not* want them in bedrooms and bathrooms, likely for privacy reasons. This underlines the observation that device preferences are location specific, and raises questions such as how do guests' views on risks to privacy change based on device location in the house, and how do they tradeoff that risk with the utility of the device; we believe these questions are worth investigating in future research.

Factor: Context. Guests' open-ended explanations indicate that their device preferences varied based on other contextual factors, such as traveling party (alone vs. family), Airbnb type (entire home vs. private room), and duration of Airbnb stay. Thus, it may be impossible to identify device preferences that meet fluid needs of guests across different contexts and areas in the house. This complication underscores the need to inform guests about the presence of devices in the Airbnb as well as their location inside the Airbnb, and to provide guests with the flexibility to disable certain devices.

5.1.3 Guests' smart device needs

Guests who wanted one or more devices in an Airbnb were asked to explain why in an open-ended response. Based on our thematic analysis of their open-ended responses, we found four themes that capture guests' smart device needs.

Entertainment. Guests sought smart TVs and gaming consoles for entertainment, for example, to occupy kids "when the adults need to unwind" or "if it is a rainy day." Some felt that these devices were "a must for any Airbnb that wants to be known for being up to modern standards." Guests liked smart TVs because they could watch streaming services and cast videos or photos from their devices.

Convenience. Guests wanted the convenience of devices such as smart doorlocks or smart lights. Many guests liked smart doorlock because they would not need to carry house keys and felt there is less risk of getting locked out in strange environments. Some guests liked smart doorlocks because they minimize interaction with the host.

> I like the digital lock because as a person with anxiety, I greatly appreciate that I can get to the rented space without having to interact with anybody. It's so much more convenient. (G84)

Luxury. Guests reported devices such as smart outlets, smart lights, smart thermostats, voice assistants were nice to have amenities. They associated these devices with a sense of comfort or luxury that made them feel good about staying in a specific Airbnb. As one guest said, "they're nice luxuries to justify the cost of staying at a nicer place." Another reported:

> [Airbnb] just made me feel I was living a luxurious lifestyle. It really felt like a vacation and still felt I was at home, much more than hotels I have stayed at. (G227)

Safety and security. Guests associated smoke sensors, door/window sensors, motion sensors, security systems, and cameras with safety and security. One guest wrote:

> I do like smart security systems as they make me feel safer in Airbnbs especially if I'm not familiar with the neighborhood and how safe it is. (G384)

Guest responses suggest that they would feel safe merely by the *presence* of security-oriented smart devices, but it is unclear whether they would want access to these devices. For instance, one guest reported that she would want a motion sensor because it "would pick up on strange things" but it is unclear whether she wanted to be alerted or expected the host to act on any alerts. This ambiguity emphasizes the need to understand people's expectations and mental models of smart devices in rental homes, and how they differ (if at all) from their expectations of smart devices in their own homes.

5.1.4 Guests' concerns

Here, we present the concerns that guests raised in their open-ended responses. Using thematic analysis, we identified four themes: spying host (n=168), discriminatory host (n=73), technically unsophisticated host (n=31), and untrustworthy device manufacturers (n=57). Note that these themes represent guests' concerns regarding what hosts *might* do if they could access certain devices or certain data types (e.g., the guest's Internet history).

Concern 1: Spying host. Guests were concerned that a host might spy on them using smart devices (e.g., smart camera, smart thermostat) if the host had access to data from these devices.

> I would just say that I have never logged on to the wifi at an Airbnb with my own device. I just don't trust giving them access to my devices or my internet activity. I also would not want a smart listening device in the rental either. If I saw one, I would disable it for my stay. (G224)

One participant elaborated that he would be uncomfortable if a host had access to his Internet activity or TV watch history because the host could learn about certain aspects of his personality (e.g., political leaning) or steal private information (e.g., credit card numbers, passwords used on websites). Note that stealing credit card numbers or passwords on major websites that use HTTPS requires a sophisticated attack and technical expertise that most hosts do not have.

Concern 2: Discriminatory host. Some participants were concerned that they would face discrimination if their behavior—monitored with smart devices—differed from other guests or was viewed unfavorably by the host. Guests were concerned that hosts would judge them, leave a bad review, or restrict their access. One participant expressed concern that hosts may judge him for his smoking habit even if he smoked only in allowed areas. Another guest participant said he needs the thermostat at a specific setting for health reasons and did not want to share this setting with hosts out of a concern for repercussions (e.g., host revoking guest's access to thermostat). A third guest who was concerned about being judged noted:

> When I use an Airbnb it is because I have a larger family 3 kids and it is difficult in a hotel. The last thing I want is for my noise level to be judged. We are going to be louder than the normal family. (G251)

Guests' open-ended explanations surfaced the nuanced role that smart devices can play in discrimination against them. Smart devices can provide reasons for discrimination (e.g., guest being too noisy, as measured with a noise meter) or serve as tools to impose retributive behaviors (e.g., restricting thermostat access). This finding highlights how smart devices can create (or increase) the power asymmetry between host and guest.

Concern 3: Technically unsophisticated host. Guests may be exposed to risks because a host lacks the ability or desire to secure smart devices (e.g., uses insecure home network access points). One guest wrote:

> I'm not comfortable with someone else's smart devices. Some people don't take the necessary security precautions and I don't want to suffer because they cant be bothered. (G224)

Another guest was concerned about hosts not changing doorlock codes between guests, which would let past guests access the house. Thus, even if guests are comfortable having smart devices in their own home, they may not be comfortable having them in Airbnbs.

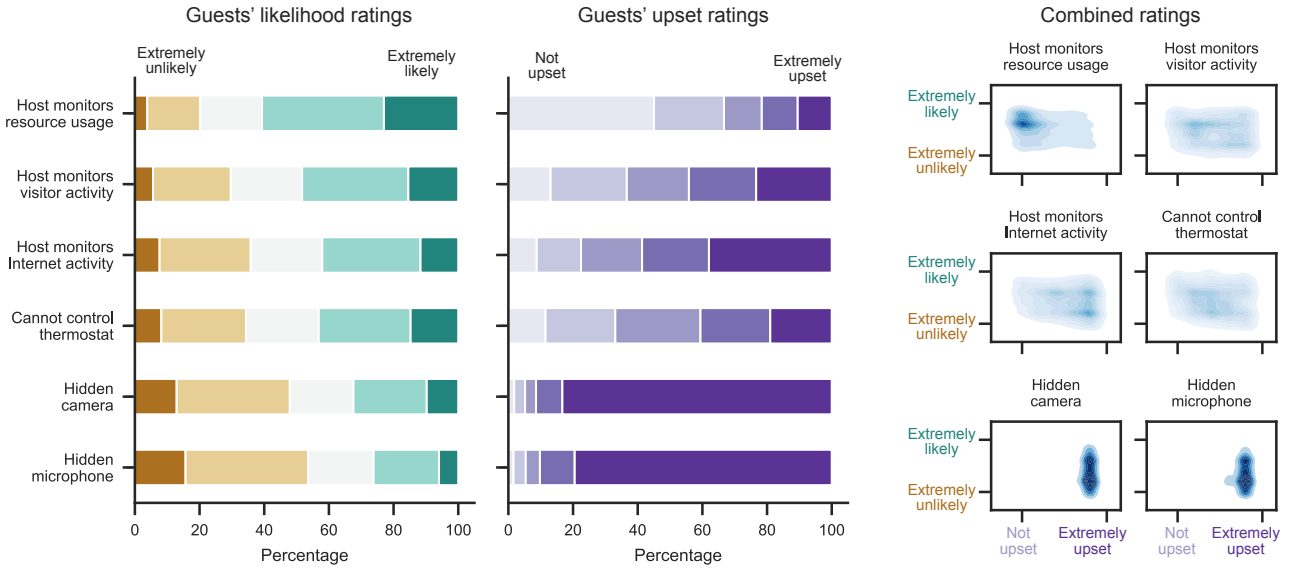

Fig. 3. Guests' likelihood and upset ratings for risk incidents in Airbnbs. (Right) guests' combined (likelihood and upset) ratings shown with probability density plots. (These density plots give a high-level snapshot of the distribution of guests' combined ratings. To illustrate, the bottom right subplot "Hidden microphone" shows that most guests reported that they would be "extremely upset" if the incident were to happen to them, but their likelihood ratings were spread between "extremely unlikely" to "likely". Figure 8 in Appendix A.4 shows a detailed plot of this distribution.)

Concern 4: Untrustworthy device manufacturers. Some guests' security and privacy concerns stemmed from their lack of trust in smart device manufacturers to ethically handle the data these devices collect or to "get security right" in these devices. Participants with such concerns, like G32, are likely not to use certain smart devices in their own homes.

> I don't trust Amazon, Google or a fair amount of the large companies because of the ways that they make their money. I also don't trust smaller manufacturers because digital security is a hard thing to do and so many companies have had severe breaches. (G32)

Risk perceptions: Likelihood and upset ratings. The guests' concerns we presented so far, based on responses to open-ended questions, shed light on guests' organic, unprompted concerns with smart devices in Airbnbs. Later in the survey, we showed guests six risk incidents that could occur in Airbnbs (Table 3), and asked them to rate each incident on a five-point likelihood scale ("extremely unlikely" to "extremely likely") and also asked them to rate how upset they would be (on a 5-point scale, "not upset" to "extremely upset") if the incident happened to them.

Whereas our thematic analysis of open-ended questions resulted in the aforementioned four key concern themes, our results in Figure 3 capture the degree of concern guests had about specific incidents, as well as how likely participants thought it would be for these incidents to manifest in Airbnbs. For the privacy-related incidents (i.e., all but thermostat control), Figure 3 suggests that in general the less likely that guests expect an incident to be, the more upset they would be if it happened to them, and vice versa. Comparing "Host monitors Internet activity" to "Cannot control thermostat," however, we see that they have similar "extremely unlikely" responses; however, more guests would be "extremely upset" if they found that a host monitored their Internet activity than if the host prevented them from controlling the thermostat. This observation suggests a potential difference in concern levels between privacy and autonomy issues, an observation that merits investigation in future research.

We next investigated how many guests both considered an incident to be extremely likely and would be extremely upset about it. We focused on hidden microphones and cameras because these incidents had the greatest number of respondents say that they would find the situations upsetting (see Appendix A for additional raw data). 4.2% of guests reported being *both* extremely upset if the hidden microphone incident were to happen to them *and* thought that hidden microphones were extremely likely to occur in Airbnbs (22 of 520); 7.1% (37 of 519) for the hidden camera incident. These numbers are even greater when we consider the 16.9% of participants who consider the hidden microphone incident to be likely (but not extremely likely) and would be ex-

tremely upset if it happened to them; 19.5% for the hidden camera. This investigation raises several questions for future work: Why do guests who would be upset over an incident that they think is likely to occur in Airbnbs still use Airbnb? Do they believe that the likelihood of risk does not apply to them when they stay in an Airbnb (e.g., because they screen hosts or choose certain types of Airbnbs)? Do they take any measures to minimize the risk? Or do they believe there is no viable safeguard against the risk?

5.2 Host findings

We now turn to the results from the host survey. We present our host participants' smart device setup, their current password practices, and their concerns and mitigation strategies.

5.2.1 Smart devices

We asked hosts which smart devices they had in their Airbnbs? Hosts were shown a list of twelve smart devices (see Table 1). Overall, we found a large variance in the number of smart devices that hosts have, with a majority of them reporting three smart devices in their Airbnb (median=3, mean=4.1, SD=3.06). The most common smart devices were smart TVs, gaming consoles, voice assistants, and smart doorlocks.

For the smart devices that hosts reported, we asked them where in the house the devices were deployed. We showed each host a house layout of their Airbnb and they could indicate device location by dragging the device on the house layout. The middle and right heatmap plots in Figure 2 show where hosts had deployed different smart devices in their Airbnbs; the middle and right heatmaps show the number of home hosts (who rent their entire home) and room hosts (who rent a private room in their home), respectively. As shown in Figure 2, host participants reported setting up smart devices in different areas of their Airbnb. A key point of note is that living rooms and bedrooms were the areas with the greatest number of smart devices, and these are also the areas that guests would access.

The dynamics of renting a private room vs. entire home are different, which suggests that there may be differences in how room hosts and home hosts use smart devices. We found minor differences in their smart device setup, i.e., the number and location of smart devices. Room hosts reported more number of smart door-

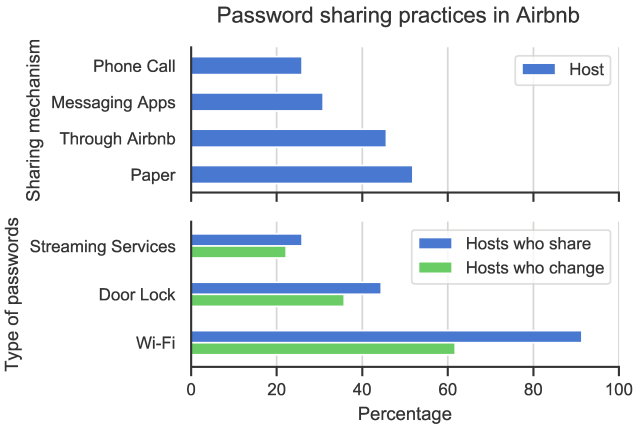

Fig. 4. Password sharing practices in Airbnb (n=82). (Top) How hosts shared passwords with guests, and (bottom) the types of passwords they shared. Hosts who reported changing passwords between guests are shown as "Hosts who change."

locks and motion sensors than home hosts. Although both types of hosts reported about the same number of smart cameras, home hosts had them primarily in the exterior areas of the house, whereas room hosts reported cameras in living room and hallway—areas that are likely shared spaces in a private room Airbnb. Due to the small sample size of hosts we cannot draw any conclusions about the differences, but recommend future work to study these differences.

5.2.2 Password management practices

During the formative stages of this study, we learned that password sharing is common in Airbnbs, and we wanted to further investigate this practice. We asked hosts which passwords they shared from four options: Wi-Fi, Streaming Services, DoorLock, and Other. We also asked how they shared passwords: Paper, Airbnb app, Messaging Apps, Phone Call, and Other.

Figure 4 shows password sharing practices reported by hosts. About 90% of hosts reported sharing Wi-Fi passwords, 43% reported sharing doorlock passcodes, and 23% reported sharing passwords for a streaming service. Hosts reported different mechanisms through which they exchanged passwords, among which writing on paper (that is then left inside the Airbnb) was the most common method. Password sharing mechanism can influence how often the password is changed or how it is chosen (e.g., digitally shared passwords are easier to change than written passwords).

Many hosts reported that they changed passwords between guest stays. About 91% of the hosts who

shared streaming service or doorlock passwords said they changed those passwords between guests, and about 67% of the hosts who shared Wi-Fi passwords said they changed it between guests. It is possible that these hosts indeed change passwords between guest stays, but we also recognize social desirability bias may be inflating these responses [11]. Regardless, these responses suggest that hosts at least think that they *should* change shared passwords. We identify a need for usable mechanisms to create, change, and share passwords for devices and services shared with guests.

5.2.3 Hosts' concerns and mitigations

We wanted to investigate hosts' concerns about guest behavior and their mitigation strategies. In particular, we wanted to know, whether hosts used smart devices to mitigate their concerns, and, if so, how. To elicit unprimed responses about concerns, we did not explicitly ask hosts to identify their concerns; instead we asked them what type of data they would want to monitor in their Airbnb during guests' stays and to explain their choices using open-ended responses. Below, we present the two main themes that we identified in our thematic analysis of their open-ended explanations.

Concern 1: Property damage, theft, and other liabilities. Hosts were concerned about any property damages caused by guests. For rentals that were in neighborhoods where break-ins were common, hosts were concerned about theft and break-ins if a guest left doors or windows open. Some hosts were concerned about being held liable if a guest did something suspicious or illegal on their property.

Mitigation strategies: Hosts did not report any viable mitigation strategy for concerns around property damage or illegal activity inside the house, but some hosts identified, and a few hosts reported using, smart cameras and motion sensors to detect break-ins.

> The only cameras I have are pointed at my front and back doors, so I feel like it'd be difficult to monitor if guests were damaging property without invading their property[sic]. The alarm system I use, however, does let me know when someone disturbs a motion sensor or leaves the house with the door unlocked. (H16)

This highlights the tension between the need to monitor the property for damage vs. respecting guests' privacy.

Concern 2: Violation of house rules. Most Airbnbs have explicit house rules for guests. Hosts reported having house rules about utility usage, pets, noise level, cleanliness, and visitors, and some hosts wanted to know when a guest breaks these rules.

Mitigation strategies: A few hosts, like H40, reported using smart cameras to catch violations of rules such as no pets, allowed of number of guests.

> A guest once brought a dog (caught him on front door security camera), which is against my house rules. I confronted him and later reported it to Airbnb. (H40)

Other rule violations—such as guest being too loud, smoking, using alcohol, or partying—are difficult to detect. Anecdotal evidence suggests some hosts drop by the Airbnb under the pretense of looking after guests, but really check on whether guests are behaving as expected.

Risk perceptions: Likelihood and upset ratings. We now present hosts likelihood and upset ratings for eight risk incident (see Figure 5). Incidents that most hosts found moderately or extremely upsetting were if a guest installed a secret camera or microphone (81%), changed a password or passcode on a device (70%), or downloaded illegal content (60%). However, many hosts also felt that these incidents were unlikely or extremely unlikely, e.g., 29% hosts thought it was extremely unlikely and 34% thought it was unlikely that a guest would install a secret camera or a microphone. This raises the question how do hosts assess the likelihood of these incidents and the associated risk to them, and how do they balance that risk with their business goals? These are important future research questions, because they would help inform hosts about risks they are unaware of and design solutions to help them better assess and manage risk.

On the other hand, a deeper analysis of the data shows that some hosts view certain situations as both extremely likely *and* extremely upsetting: 11.1% of hosts would be extremely upset if guests misused resources *and* considered such misuse extremely likely; 9.3% for the downloading illegal content scenario; 5.7% for breaking house rules; 4.4% for leaving doors/windows unlocked (see Appendix A.4 for additional raw data). For at least some hosts, these percentages suggest that there would be a strong incentive to monitor or prevent undesirable actions by guests. A key question, which we turn to in Section 6, is whether it is possible to enable such monitoring while minimizing negative privacy impacts on guests.

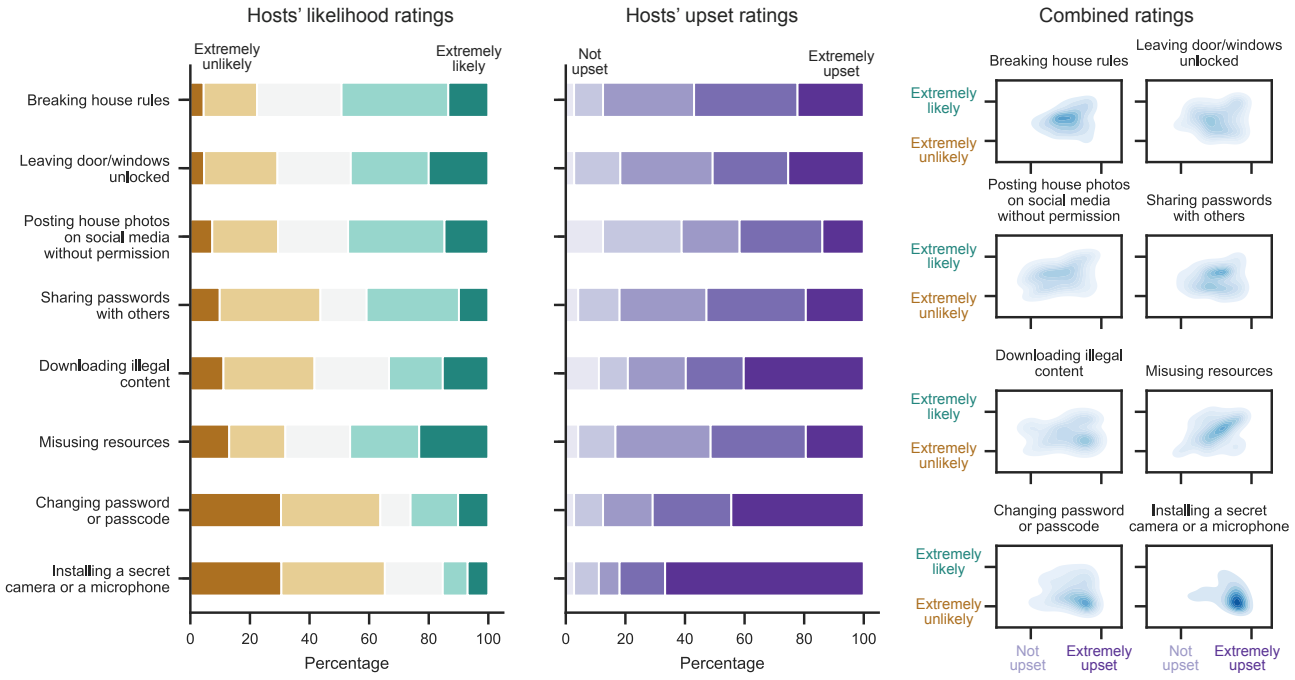

Fig. 5. Hosts' likelihood and upset ratings for risk incidents in Airbnb. (Right) Hosts' combined (likelihood and upset) ratings shown with probability density plots (n=82). (The density plots give a high-level distribution of hosts' combined ratings; Figure 9 in Appendix A.4 shows a detailed plot of this distribution.)

5.3 Comparing views of guests and hosts

We now step back from individual findings of guests and hosts to compare their views on information sharing, smart devices, and trust in Airbnbs.

Views on information sharing. Data collection and sharing preferences are potential tension points between guests and hosts: what data do hosts want, and what data are guests willing to share with hosts?

The left plot in Figure 6 shows the data collection and sharing preferences of hosts and guests for eleven different data types. Guests, on average, were more comfortable sharing house-related data (e.g., thermostat setting) than their personal data (e.g., visitor activity). We also found that, on average, guests were comfortable sharing more data than our hosts wanted. For instance, 43% of guests were comfortable sharing their TV watching history, but only 12% of hosts wanted that data; 48% of guests were comfortable sharing their visitor activity, while 33% of hosts wanted that data. These aggregate results raise the question: are guests' and hosts' data sharing preferences actually compatible in a way that makes it unlikely for hosts to violate guests' data sharing preferences?

Although, in aggregate, the *world view* of guests and hosts about information sharing may appear compatible, there is currently *no* guarantee that a guest would stay with a host that had compatible preferences. A host who wants to monitor Internet history may get a guest uncomfortable with sharing this history—an incompatible match. From a privacy perspective, an important question is: what are the chances of such incompatible matches? The left plot in Figure 6 shows a list of data types, and for each data type, the fraction of guests who do not want to share that data with hosts. For such a guest, the right plot (heatmap) in Figure 6 shows the expected number of times the guest's privacy preference would be violated across different numbers of Airbnb stays, assuming the guest selects hosts uniformly at random. To approximate the probability that a host would collect certain information we used host responses. For example, consider the data "Number of guests staying." About 50% hosts want this data, but 23% of our guest participants did not want to share this data with hosts. If one of these 23% guests stayed with hosts in our sample, their privacy could on average be violated after 2 stays. As shown in Figure 6, within two Airbnb stays the guest's privacy with respect to four (of 11) data types would be violated, and by eight Airbnb stays, the guest's privacy with respect to all data types would be violated.

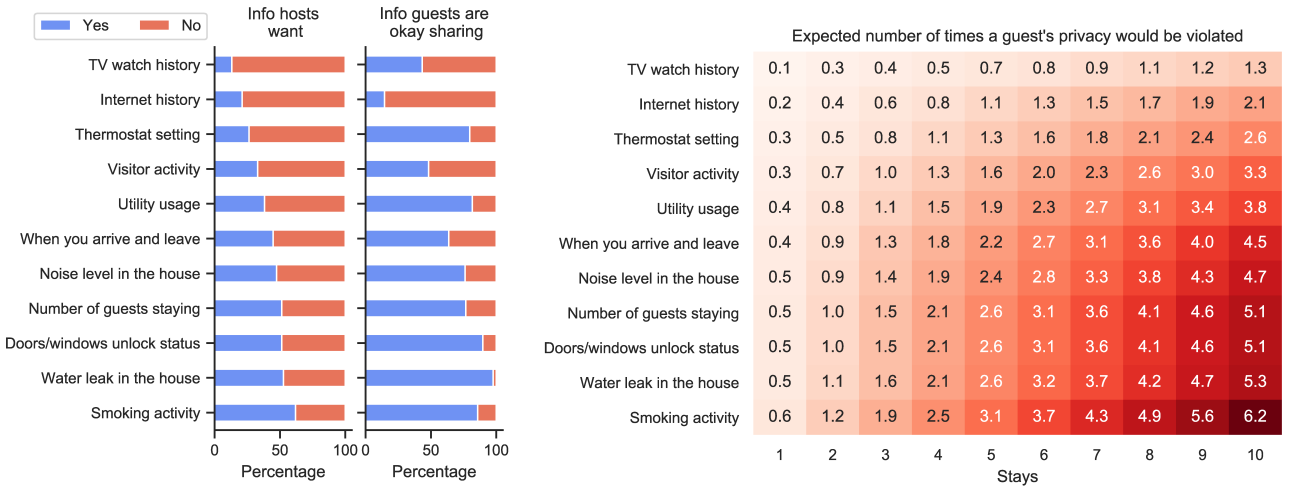

Fig. 6. (Left) Information sharing views of guests and hosts. (Right) If a guest does not want to share information with hosts, the right plot shows the expected number of times the guest's information sharing preference would be violated across number of Airbnb stays, assuming the guest selects hosts uniformly at random.

Views on smart devices. We found that, on average, smart device preferences of guests and hosts were aligned for devices related to entertainment, utility, and safety; in particular, smart TVs, smart doorlocks, gamings consoles, smart smoke sensors, and smart thermostats (Figure 1 and Section 5.1.1). Guest and host preferences differed the most for the smart devices that many guests considered as potentially privacy-violating devices—smart cameras, motion sensors, and voice assistants.

For these three potentially privacy-violating devices, guest and host preferences also differed about the appropriate location to place these devices in a house (Figure 2). Guests indicated that the least objectionable place for smart cameras, motion sensors, and voice assistants were the front/back yard and kitchen, but some hosts had these devices in the living room, which many guests considered private. This suggests that even though both a host and a guest may agree on the presence of a smart device in an Airbnb, they may not agree on its location.

6 Design recommendations

Informed by our findings, we now synthesize suggestions for future design and research of smart home technology to address the privacy and security tensions between well-meaning, non-malicious guests and hosts.

(R1) Least privilege sensing. We found that one of the main reasons hosts use smart devices is to know when guests violate house rules (Section 5.2.3). Commonly available smart devices can provide hosts with the information they need, but these devices also capture additional information that hosts may neither need nor want (e.g., a microphone captures noise level, which hosts may want, but it also captures conversation content). This additional information may pose undue privacy risks for guests.

We suggest that smart home designers consider creating software or hardware abstractions that use the well-known principle of least privilege [36, 37] to restrict a host's smart device access to *only* the information that the host legitimately needs *during* a guest's stay, and give the host unrestricted access when there are no guests. For example, a smart camera with a pet-detector software layer could notify the host if a guest brings a pet instead of giving the host access to raw video during a guest's stay; to detect noise, a sound sensor with a hardware layer that measures only sound level (in decibels) may offer more privacy and security than a microphone that also records conversations. Such abstractions could operate on one smart device or a set of smart devices in a home. In designing abstraction layers, open research questions include how to identify and develop the needed abstractions; how to provide these abstractions to hosts; whether a guest should be allowed to enable these abstractions for devices in Airbnbs; and how to assure guests that abstractions are correctly enforced. Recent work on limiting sensory information to preserve privacy (e.g., limiting video feed [22]) could be leverage to tackle some of these questions.

(R2) Smart home dashboard for guests. Currently, guests have no visibility on the data that smart devices collect about them during their Airbnb stay. Even if they are aware about the presence of a smart device in the Airbnb, we found that if a host confronts a guest for breaking a house rule based on the data from the smart device, guests find that "creepy" and uncomfortable because they feel they are "being watched". To inform and remind guests about any smart devices in the house and what data they collect, we propose creating a smart home dashboard for guests. Such a dashboard could show guests relevant information about the devices in the Airbnb and provide an interface to control them. However, to determine what relevant information should be shared requires careful consideration because some guests could misuse the information to break house rules without being detected.

(R3) Access control and home reset. We found that hosts share two-to-three different types of access credentials with guests, and they change (or want to change) the credentials between guest stays (Section 5.2.2). As smart devices become more prevalent, hosts' need to share access with guests will likely increase. Smart home designers and home sharing platform developers should consider unifying access to different smart devices and services (e.g., streaming services) into a single access, which could be, for example, a central service that manages passwords and accounts, or an OAuth derivative.

Many hosts, like our participants, routinely do manual tasks between guests such as creating access (e.g., doorlock) for future guests, revoking access for past guests, making sure all devices are connected and configured properly (e.g., guests may unplug devices or log out of the host's streaming account on a smart TV). A smart home reset option that automates these manual tasks could be beneficial to hosts.

(R4) Trusted third-party Wi-Fi. Host-provided Wi-Fi in Airbnbs is a source of tension between guests and hosts (Section 5.3). This tension could be reduced by using a Wi-Fi provided by a third-party trusted by both hosts and guests. Airbnb Inc. could potentially serve as that trusted party and provide "Airbnb Wi-Fi" using inexpensive RADIUS-enabled routers and providing the necessary centralized authentication and authorization server [1]. Airbnb Wi-Fi could be attractive to both guests and hosts: guests can simply use their Airbnb credentials to access Airbnb Wi-Fi and be confident that their Internet history is protected from the host; and a third-party Wi-Fi could mitigate hosts' concerns about Wi-Fi access management and liability due to guests' Internet activity. Although there is precedence of third-party Wi-Fi in coffee shops and other public places (e.g., Google Wi-Fi), it is important to carefully consider privacy implications and user reactions for a centralized third-party Wi-Fi service in Airbnbs.

(R5) Responsible device disclosure. We found that the current Airbnb Host Safety guidelines [3] are inadequate for addressing guest concerns about device disclosure (Section 5.1.4). An important takeaway from our study is the strong need for comprehensive guidelines for responsible smart device disclosure—*what* to disclose and *how*—so that guests can make informed decisions when choosing an Airbnb and during their stay.

What to disclose? We suggest disclosing *every* smart device that collects data about guests because it is likely, as we found (Section 5.1), that for any smart device some guests want it while others do not. Guests, like our participants, may want to know more about each device: what the device collects; device location in the house; whether guests can turn off the device, and how; and whether guests are allowed to use the device. Some participants also wanted to know what the device is used for (and by whom), which echoes prior work that states people care about intended use of data [28].

How to disclose? This open research question has three main challenges. First, how can all device disclosure information be displayed in a way that guests can easily understand to make informed privacy decisions? A potential approach, building on recent work [33], is to create a "smart home label"—similar to nutrition labels that are familiar to consumers, but for the entire smart home rather than individual IoT devices. Second, how should the information be disclosed so guests can trust (ideally, verify) its accuracy? Third, how can the information be disclosed without increasing security risks for hosts? Because publicly disclosing information about certain smart devices (e.g., security system, security cameras) could pose security risk to hosts.

(R6) Smart home profiles. Many hosts reported deploying voice assistants in common areas where guests can also access these devices. Voice assistants offer personalized recommendations and may also allow access to personal services (e.g., calendar, messages). So a shared use of voice assistants, particularly in shared homes, creates a privacy-utility tension. When a host's voice assistant is used by guests, it may leak the host's private information or affect future recommendations for the host. Conversely, hosts may be able to learn about guests' in-

teraction with a voice assistant, a potential privacy violation for guests. We suggest developing smart home profiles that can inform smart devices about changes in home context, enabling smart devices to adapt their behavior accordingly. For example, in a *host* profile, the host's voice assistant could read a host's messages and give personalized recommendations, but in a *guest* profile, the voice assistant would not access any of the host's personal accounts, would provide non-personalized recommendations, and would not save any interactions to reduce guest privacy risks. The concept of profiles is extensively used in apps (e.g., browsers), devices (e.g., Xbox, Android tablet), and services (e.g., Netflix), and can be leveraged when designing smart home profiles.

7 Discussion

In addition to the specific open research and design questions in Section 6, we consider two broader research challenges surfaced in our findings.

Trust among users of home sharing platforms. Trust between hosts and guests is crucial for a home sharing platform like Airbnb. When a home sharing community (in fact, any sharing community) is small, just being a member of the community is a sign of trustworthiness within the community, simply because members in a small community are usually the people who share the community values. As a community grows and people who do not share the same values (e.g., opportunity-seekers) join, community membership no longer implies trustworthiness [7]. As the home sharing community grows, maintaining trust within the community becomes challenging. Thus, the broader research questions include: How can technology support and help build trust relationships between users of a home sharing platform? What defines trustworthiness for guests and hosts? How can one improve perceived trustworthiness? How can these goals be accomplished while accounting for the needs, concerns, and issues raised in this work (Section 5)?

Mental models of shared smart homes. From a guest's perspective, smart devices in shared home are installed by a stranger (host) who has access to the device data and may share that data with other parties. Guests may encounter smart devices that they avoid at home or are unfamiliar to them (and have not formed any mental models about those devices). Furthermore, as our findings suggest (Section 5.1.3), participants may associate the presence of certain devices with certain behavior and expectations (e.g., motion sensor will detect intruders). Recent work indicates that people find it challenging to create correct mental models of smart devices in their own homes [43–45]. We hypothesize that it will become even more challenging for people to do so when they are guests in someone else's house or when they host strangers in their house. Unfortunately, as is well known [6, 40], incorrect or incomplete mental models lead to poor privacy and security decisions. Thus, future research should strive to both better understand the gaps in guests' mental models of smart devices in shared homes and help scaffold correct mental models.

8 Conclusion

The use of smart home devices in a shared home, like Airbnb, poses privacy and security implications for both hosts and guests. To better understand these implications, in the context of Airbnb we studied current smart device practices, hosts' and guests' preferences for smart devices in shared home, and their perceptions of risks due to the use of smart devices in Airbnbs. Through a survey of 82 hosts and 554 guests, we surfaced several tensions between guests and hosts. We found, for example, that both guests and hosts largely want smart devices in Airbnbs, but guests were concerned about their privacy and autonomy implications. Hosts wanted to use smart devices to deter and detect guest misbehavior, but their ad hoc ways of using smart devices pose privacy risks for guests. We developed recommendations to address such tensions and suggest opportunities for future research.

9 Acknowledgements

We thank our survey participants and testers for their valuable input. We thank our shepherd, Lujo Bauer, as well as our anonymous reviewers for their insightful feedback. We are grateful to Karl Koscher for his help in developing the interactive web survey, and to Camille Cobb, Ivan Evtimov, Christine Geeng, Clarice Larson, and Nigini Oliveira for their feedback on the initial versions of the survey. We also thank Earlence Fernandes and Sandy Kaplan for their helpful feedback on earlier drafts of this paper. This work was supported in part by the National Science Foundation under awards CNS-1513584, CNS-1565252, and CNS-1565375.

References

[1] Wi-Fi security with RADIUS. Last accessed November 2019, Online at https://networkradius.com/blog/security/wifi-security-with-radius/index.html.

[2] *Handbook of Survey Research*. Elsevier, 1983. DOI 10.1016/C2013-0-11411-0.

[3] Airbnb hosting safety. Last accessed May 2019, Online at https://www.airbnb.com/help/article/887/what-are-airbnb-s-rules-about-electronic-surveillance-devices-in-listings.

[4] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. SoK: Security evaluation of home-based IoT deployments. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2019. DOI 10.1109/SP.2019.00013.

[5] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, January 2006. DOI 10.1191/1478088706qp063oa.

[6] L. Jean Camp. Mental models of privacy and security. *IEEE Technology and Society Magazine*, 2009. DOI 10.1109/MTS.2009.934142.

[7] Filippo Celata, Cary Yungmee Hendrickson, and Venere Stefania Sanna. The sharing economy as community marketplace? Trust, reciprocity and belonging in peer-to-peer accommodation platforms. *Cambridge Journal of Regions, Economy and Society*, 10(2), 2017. DOI 10.1093/cjres/rsw044.

[8] Mingming Cheng and Xin Jin. What do Airbnb users care about? An analysis of online review comments. *International Journal of Hospitality Management*, 76, January 2019. DOI 10.1016/j.ijhm.2018.04.004.

[9] Yushi Cheng, Xiaoyu Ji, Tianyang Lu, and Wenyuan Xu. On detecting hidden wireless cameras: A traffic pattern-based approach. *IEEE Transactions on Mobile Computing*, 2019. DOI 10.1109/TMC.2019.2900919.

[10] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. Living in a glass house: A survey of private moments in the home. In *Proceedings of the International Conference on Ubiquitous Computing (UbiComp)*. ACM, 2011. DOI 10.1145/2030112.2030118.

[11] Douglas P. Crowne and David Marlowe. A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology*, 24(4), 1960. DOI 10.1037/h0047358.

[12] Edward E. Cureton. Rank-biserial correlation. *Psychometrika*, 21(3), September 1956. DOI 10.1007/BF02289138.

[13] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. Computer security and the modern home. *Commununications of the ACM*, 56(1), January 2013. DOI 10.1145/2398356.2398377.

[14] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. Security analysis of emerging smart home applications. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, May 2016. DOI 10.1109/SP.2016.44.

[15] Andrey Fradkin, Elena Grewal, and David Holtz. The determinants of online review informativeness: Evidence from field experiments on Airbnb. SSRN Scholarly Paper ID 2939064, April 2018. Online at https://papers.ssrn.com/abstract=2939064.

[16] Christine Geeng and Franziska Roesner. Who's in control?: Interactions in multi-user smart homes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2019. DOI 10.1145/3290605.3300498.

[17] Eric A. Greenleaf. Measuring extreme response style. *The Public Opinion Quarterly*, 56(3), 1992. Online at https://www.jstor.org/stable/2749156.

[18] Airbnb: Vacation rentals, homes, experiences & places. Online at https://www.airbnb.com/.

[19] HomeExchange – #1 home exchange community. Online at https://www.homeexchange.com/.

[20] Homestay accommodation worldwide for short and long term stays. Online at https://www.homestay.com/.

[21] Utility smart meter installations worry Rockland and Westchester homeowners on privacy. Last accessed May 2019, Online at https://www.lohud.com/story/news/2018/11/14/smart-meters-pose-privacy-worries-homeowners-o-and-r-con-ed/1823505002/.

[22] Suman Jana, Arvind Narayanan, and Vitaly Shmatikov. A scanner darkly: Protecting user privacy from perceptual applications. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, May 2013. DOI 10.1109/SP.2013.31.

[23] Airi Lampinen and Coye Cheshire. Hosting via Airbnb: Motivations and financial assurances in monetized network hospitality. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2016. DOI 10.1145/2858036.2858092.

[24] Josephine Lau, Benjamin J 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 (PACM HCI)*, 2(CSCW), 2018. DOI 10.1145/3274371.

[25] Paul Lavrakas. *Encyclopedia of Survey Research Methods*. Sage Publications, Inc., 2008. DOI 10.4135/9781412963947.

[26] Xiao Ma, Jeffrey T. Hancock, Kenneth Lim Mingjie, and Mor Naaman. Self-disclosure and perceived trustworthiness of Airbnb host profiles. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*, 2017. DOI 10.1145/2998181.2998269.

[27] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "What can't data be used for?" Privacy expectations about smart TVs in the U.S. In *Proceedings of the European Workshop on Usable Security (EuroSEC*, 2018. DOI 10.14722/eurousec.2018.23016.

[28] Kirsten E. Martin and Helen Nissenbaum. Measuring privacy: An empirical test using context to expose confounding variables. SSRN Scholarly Paper ID 2709584, Social Science Research Network, December 2015. Online at https://papers.ssrn.com/abstract=2709584.

[29] Airbnb statistics for demographics and growth. Last accessed February 2019, Online at https://ipropertymanagement.com/airbnb-statistics/.

[30] Airbnb's impact on hotels, 2015. Last accessed November 2019, Online at http://res.cloudinary.com/yumyoshojin/image/upload/v1/pdf/future-of-hospitality.pdf.

[31] Important reasons why people use Airbnb in the United States and Europe from 2015 to 2017, 2017. Last accessed November 2019, Online at https://www.statista.com/statistics/796866/reasons-people-use-airbnb/.

[32] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman M. Sadeh. Privacy expectations and preferences in an IoT world. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2017. Online at https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini.

[33] 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 SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2019. DOI 10.1145/3290605.3300764.

[34] Will Qiu, Paolo Parigi, and Bruno D. Abrahao. More stars or more reviews? Differential effects of reputation on trust in the sharing economy. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2018. DOI 10.1145/3173574.3173727.

[35] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. A summary of survey methodology best practices for security and privacy researchers, 2017. DOI 10.13016/M22K2W.

[36] Fred B Schneider. Least privilege and more. *IEEE Security & Privacy*, 99(5), 2003. DOI 10.1109/MSECP.2003.1236236.

[37] Richard E Smith. A contemporary look at Saltzer and Schroeder's 1975 design principles. *IEEE Security & Privacy*, 10(6), 2012. DOI 10.1109/MSP.2012.85.

[38] Sara Sorcher. The Technology 202: Alexa, are you spying on me? Here's why smart speakers raise serious privacy concerns. The Washington Post, May 2019. Online at https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/05/06/the-technology-202-alexa-are-you-spying-on-me-here-s-why-smart-speakers-raise-serious-privacy-concerns/5ccf46a9a7a0a46cfe152c3c/.

[39] Aron Szanto and Neel Mehta. A host of troubles: Re-identifying Airbnb hosts using public data. Technology Science, October 2018. Online at https://techscience.org/a/2018100902.

[40] Rick Wash. Folk models of home computer security. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2010. DOI 10.1145/1837110.1837125.

[41] Molly Wood. CES: Security risks from the smart home. The New York Times, January 2018. Online at https://www.nytimes.com/2015/01/08/technology/personaltech/ces-security-risks-from-the-smart-home.html.

[42] Kevin Wu and Brent Lagesse. Do you see what I see? Detecting hidden streaming cameras through similarity of simultaneous observation. *CoRR*, abs/1901.02818, 2019. Online at http://arxiv.org/abs/1901.02818.

[43] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2017. Online at https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng.

[44] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction (PACM HCI)*, 2(CSCW), November 2018. DOI 10.1145/3274469.

[45] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. Home, smart home – Exploring end users' mental models of smart homes. In Raimund Dachselt and Gerhard Weber, editors, *Mensch und Computer 2018 - Workshopand*. Gesellschaft für Informatik e.V., 2018. DOI 10.18420/muc2018-ws08-0539.

A Appendix

A.1 Screening Survey

Q1) Which of the following online services do you use?
- (1) Google
- (2) Twitter
- (3) Airbnb
- (4) Facebook
- (5) LinkedIn
- (6) Uber
- (7) VRBO

Q2) Which of the following services have you used?
- (1) Airbnb
- (2) Hotel
- (3) Hostel
- (4) Vacation Rentals (VRBO)
- (5) Homestay
- (6) Some home rental service

Q3) Are you an Airbnb host or guest?
- (1) Host
- (2) Guest
- (3) Both

A.2 Guest Survey

Q1) How many Airbnbs in total have you stayed in so far?
- (1) Less than 5
- (2) 5-10
- (3) 11-20
- (4) More than 20

Q2) When was the last time time you stayed in an Airbnb?
- (1) Less than 3 months ago
- (2) 3-6 months ago
- (3) 7-12 months ago
- (4) More than 1 year ago

Q3) Thinking back to all your Airbnb stays, which type of Airbnbs have you stayed in?
- (1) Private room
- (2) Shared room
- (3) Entire place

Q4) Thinking back to the Airbnbs you visited, which of the following smart devices/things have you noticed in Airbnbs?
- (1) Digital Door Lock (e.g., lock with a keypad)

(2) Door/Window Sensor
(3) Gaming Console (e.g., Xbox, PlayStation)
(4) Motion Sensor
(5) Smart Camera (e.g., Nest camera)
(6) Smart Light (e.g., Philips Hue lights)
(7) Smart Power Outlet
(8) Smart Security System (e.g., ADT)
(9) Smart Smoke Sensor (e.g., NEST smoke sensor)
(10) Smart Thermostat (e.g., Nest thermostat)
(11) Smart TV (e.g., TV with Wi-Fi)
(12) Voice Assistant (e.g., Amazon Echo)
(13) Other

Q5) You mentioned you have noticed the following smart devices in Airbnbs. Which of these devices have you used during your stay at an Airbnb? *(Options for this question were things participant chose in question Q4.)*

Q6) Thinking back to your Airbnb stays, did any host provide the following services?
(a) TV streaming services (e.g., Netflix)
(b) Internet (Wi-Fi or wired)
(c) Music streaming services (e.g., Spotify)
(d) Camera set up to call host

Q7) You mentioned some Airbnb hosts provided the following services. Did you use the service during your stay at those Airbnbs? *(Options for this question were things participant chose in question Q6.)*

Q8) Imagine someone creating a new Airbnb rental. For the following devices, please indicate whether you (as a guest) would like to have these devices in an Airbnb.
(1) Digital Door Lock (e.g., lock with a keypad)
(2) Door/Window Sensor
(3) Gaming Console (e.g., Xbox, PlayStation)
(4) Motion Sensor
(5) Smart Camera (e.g., Nest camera)
(6) Smart Light (e.g., Philips Hue lights)
(7) Smart Power Outlet
(8) Smart Security System (e.g., ADT)
(9) Smart Smoke Sensor (e.g., NEST smoke sensor)
(10) Smart Thermostat (e.g., Nest thermostat)
(11) Smart TV (e.g., TV with Wi-Fi)
(12) Voice Assistant (e.g., Amazon Echo)
(Participants were asked to vote for each device on a 4-point scale: Yes, Neutral, Depends, and No)

Q9) If participant selected "Yes" for any device in Question 8, they were asked to elaborate why they want those devices in Airbnb.

Q10) If participant selected "No" for any device in Question 8, they were asked to elaborate why they would not want those devices in Airbnb.

Q11) If participant selected "Depends" for any device in Question 8, they were shown a house layout and asked to indicate where in the house they would not want the devices. Figure 10 in Appendix A.4 shows the a screenshot of this question.

Q12) Some hosts like to monitor their Airbnb to prevent any misuse. Please indicate which of the following activity/information you would prefer NOT TO SHARE with your Airbnb host.
(1) When you arrive and leave
(2) Internet history (e.g., sites visited)
(3) Noise level in the house
(4) Number of guests staying
(5) Smoking activity
(6) Thermostat setting
(7) TV watching history
(8) Doors/windows unlock status
(9) Utility usage (e.g., electricity, heat, water)
(10) Visitor activity
(11) Water leak in the house
(12) Other

Q13) How likely do you think it is for the following incidents to happen in Airbnbs?
(1) A hidden audio recording devices
(2) A hidden camera
(3) Host monitoring guest Internet activity (e.g., sites visited, files downloaded)
(4) Host monitoring visitor activity (e.g., people visiting you)
(5) Host monitoring resource usage in Airbnb (e.g., electricity, water usage)
(6) Guest not allowed to control thermostat (e.g., Host installs a smart thermostat that only they can control)
(For each incident, participants had to choose on a 5-point likert scale: extremely unlikely -to- extremely likely.

Q14) If the following incidents were to happen to you, how would you feel?
(1) A hidden audio recording devices
(2) A hidden camera
(3) Host monitoring guest Internet activity
(4) Host monitoring visitor activity
(5) Host monitoring resource usage in Airbnb
(6) Guest not allowed to control thermostat
(For each incident, participants had to choose on a 5-point likert scale: not at all upset -to- extremely upset.

Q15) How do you communicate with hosts?
(1) Messages with Airbnb
(2) Text messages (SMS, MMS)
(3) Apple iMessages
(4) Smartbnb
(5) WhatsApp
(6) Phone Call
(7) Facebook Messenger
(8) Email
(9) Depends on what the host uses
(10) Other

Q16) Did any host ever share any passwords or passcodes with you?

Q17) Which passwords or passcodes do you recall hosts sharing with you?
(1) Wi-Fi
(2) Streaming Services
(3) Door Lock

(4) Other

Q18) How did hosts share passwords or passcodes with you?
(1) Writing on paper/sticky notes
(2) Through Airbnb (e.g., using Airbnb listing or Airbnb account)
(3) Messaging Apps (e.g., WhatsApp, Apple iMessages)
(4) Phone Call
(5) Other

Q19) When you check in to your Airbnb rentals, is there something that you always do?

Q20) Why do you use Airbnb rentals?

Q21) Have you had any bad experience when staying at an Airbnb?

Q22) Can you briefly share your most memorable bad experience?

Q23) Is there anything else you would like to share about your Airbnb experience?

A.3 Host Survey

Q1) Do you host a home or an experience?
(1) Home (or room in a home)
(2) Experience
(3) Both
(The rest of the survey was shown only to participants who chose (1) or (3) in this question.)

Q2) Do you own or manage your Airbnb?
(1) Own
(2) Manage
(3) Both

Q3) How many Airbnbs do you currently own or manage?
(1) 1
(2) 2
(3) 3
(4) 4 or more

Q4) What is the type of your Airbnb?
(1) Private room
(2) Shared room
(3) Entire home

Q5) In which country is your Airbnb located?

Q6) Is the Airbnb your primary home or your secondary home?
(1) Primary home
(2) Secondary home
(3) Other

Q7) Is the Airbnb room in a home that you live in? (Yes/No)

Q8) Why do you rent your space through Airbnb?
(1) To earn some extra money
(2) To have a stable secondary income
(3) It is my primary source of income
(4) To meet different people
(5) Other

Q9) How many of the following rooms/areas are there in your Airbnb house?
(1) Bathroom
(2) Bedroom
(3) Doors/Windows
(4) Front/Back Yard
(5) Hallway
(6) Kitchen
(7) Living Room
(8) Store Room
(9) Study Room
(For each of the options above, participants could choose one of three options: (i) 0 (ii) 1 (ii) 2+ (2 or more).)

Q10) Which of the following devices do you have in your Airbnb house?
(1) Digital Door Lock (e.g., lock with a keypad)
(2) Door/Window Sensor
(3) Gaming Console (e.g., Xbox, PlayStation)
(4) Motion Sensor
(5) Smart Camera (e.g., Nest camera)
(6) Smart Light (e.g., Philips Hue lights)
(7) Smart Power Outlet
(8) Smart Security System (e.g., ADT)
(9) Smart Smoke Sensor (e.g., NEST smoke sensor)
(10) Smart Thermostat (e.g., Nest thermostat)
(11) Smart TV (e.g., TV with Wi-Fi)
(12) Voice Assistant (e.g., Amazon Echo)
(13) Other

Q11) Please mark the areas in your house (by clicking on them) that you DO NOT want your Airbnb guests to enter or have access to. *(Participants were show a rough layout of their house, using their response to Q9.)*

Q12) Where are the smart devices in your house? Show by dragging devices to appropriate rooms/areas. *(Participants were show a list of smart devices they chose in Q10.)*

Q13) If cost was not an issue, would you buy any new smart devices for your Airbnb?
(1) Yes
(2) No
(3) Maybe

Q14) If cost was not an issue, which of the following smart devices would you get and where would you keep them in your Airbnb? Show by dragging devices to the rooms/areas where you would keep them. *(Participants were show a list of all smart devices; the devices they already have were shown with a different color.)*

Q15) How do you communicate with guests?
(1) Messages with Airbnb
(2) Text messages (SMS, MMS)
(3) Apple iMessages
(4) Smartbnb
(5) WhatsApp
(6) Phone Call
(7) Facebook Messenger
(8) Email
(9) Depends on what the host uses

(10) Other

Q16) Which passwords or passcodes (if any) do you share with guests?
(1) Wi-Fi
(2) Streaming Services
(3) Door Lock
(4) Other

Q17) How do you share passwords or passcodes with guests?
(1) Writing on paper/sticky notes
(2) Through Airbnb (e.g., using Airbnb listing or Airbnb account)
(3) Messaging Apps (e.g., WhatsApp, Apple iMessages)
(4) Phone Call
(5) Other

Q18) Select all the passwords or passcodes that you change between guests
(1) Wi-Fi
(2) Streaming Services
(3) Door Lock
(4) Other

Q19) Some Airbnb hosts like to monitor their rental to prevent any misuse. Which of the following activity/information would you like to monitor in your Airbnb space?
(1) When guests arrive and leave
(2) Internet history (e.g., sites visited)
(3) Noise level in the house
(4) Number of guests staying
(5) Smoking activity
(6) Thermostat setting
(7) TV watching history
(8) Doors/windows unlock status
(9) Utility usage (e.g., electricity, heat, water)
(10) Visitor activity
(11) Water leak in the house
(12) Other

Q20) Following are some incidents that some Airbnb hosts are concerned about. How likely do you think these will happen to you? *(Participants were asked to rate each incident on a 5-point scale: Extremely unlikely, Unlikely, Neutral, Likely, and Extremely likely)*
(1) Guest breaking house rules
(2) Guest changing password or passcode on devices (e.g., router)
(3) Guest downloading illegal content on Internet
(4) Guest installing a secret camera or a microphone
(5) Guest leaving door/windows unlocked
(6) Guest logging out of your account (e.g., Netflix, Hulu)
(7) Guest misusing resources (or using excessively)
(8) Guest posting house photos on social media without permission
(9) Guest sharing passwords with others

Q21) If the following incidents were to happen to you, how would you feel? *(Same options as Q20. Participants were asked to rate each incident on a 5-point scale: Not at all upset, Slightly upset, Somewhat upset, Moderately upset, and Extremely upset)*

Q22) Do you offer TV streaming services (e.g., Netflix, Amazon Prime, Hulu) to guests? (Yes/No)

Q23) Did any of your guests accidentally leave their streaming service account logged in on your TV?
(1) Yes
(2) No
(3) I'm not sure
(4) N/A (there is no TV in my Airbnb)

Q24) The streaming service(s) account that you share with guests, is it your personal account or a special account made only for Airbnb?
(1) Special account only for Airbnb
(2) Personal account
(3) Other

Q25) How do you give guests access to streaming service(s)?
(1) I set up TV with streaming services (e.g., sign in Netflix) before guests arrive,
(2) I share streaming service password with guests,
(3) Other

Q26) What do you do when a guest accidentally logs out of the streaming service account setup on the TV?

Q27) Did you have any bad experience with guests? (Yes/No)

Q28) Can you briefly share your most memorable bad experience?

Q29) Is there anything else you would like to share about your Airbnb experience?

A.4 Additional Data

In this appendix we present additional data. This data is not necessary to understand the body of this paper. Instead, this data complements the results presented in the body of the paper. This additional data is captured in Figure 7, Figure 8, Figure 9, and Figure 10.

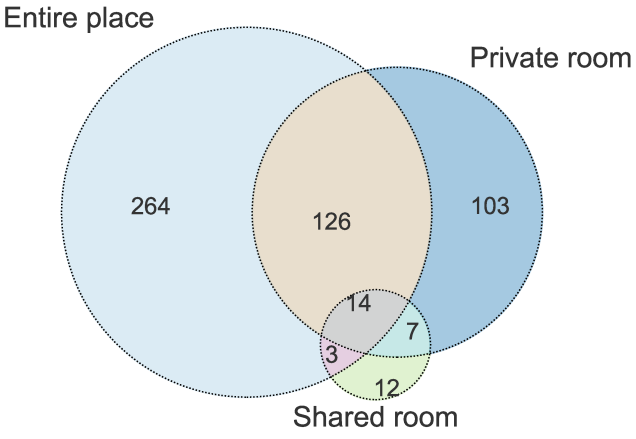

Fig. 7. The types of Airbnb rented by our guest participants.

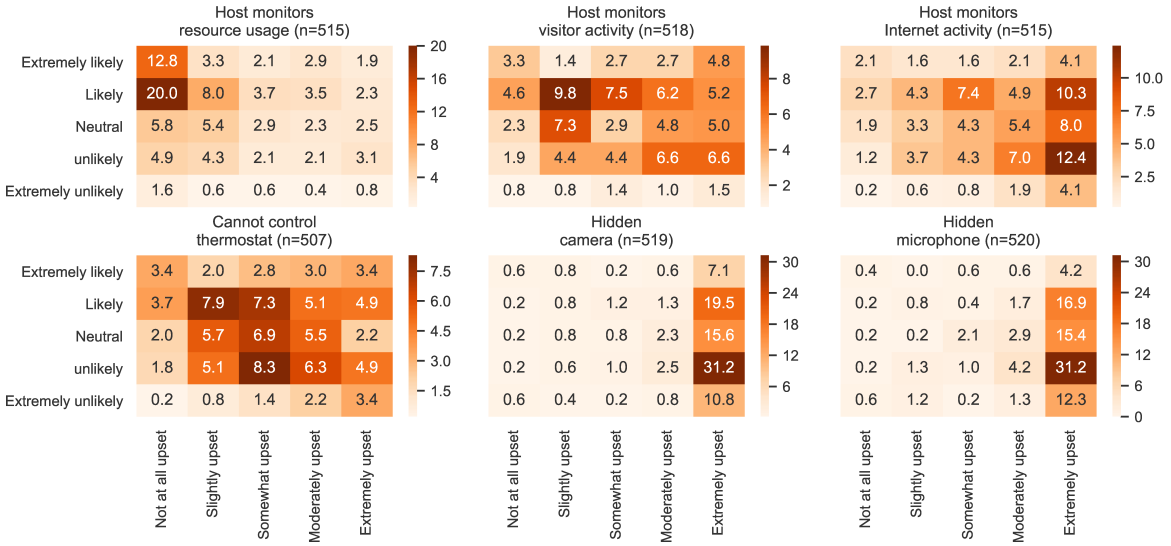

Fig. 8. Each subplot shows a heatmap of guests' likelihood and upset ratings for one incident (given in subplot title) that can occur in Airbnbs. Rows represent likelihood rating and columns represent upset ratings. In a subplot, the number in each cell shows the percentage of guests who gave a likelihood rating represented by the row and upset rating represented by the column. For instance, in subplot "Host monitors visitor activity," the value 3.3 in the top left cell indicates that 3.3% guests rated the incident "Host monitors visitor activity" as *extremely likely* (row) and gave an upset rating of *not at all upset* (column).

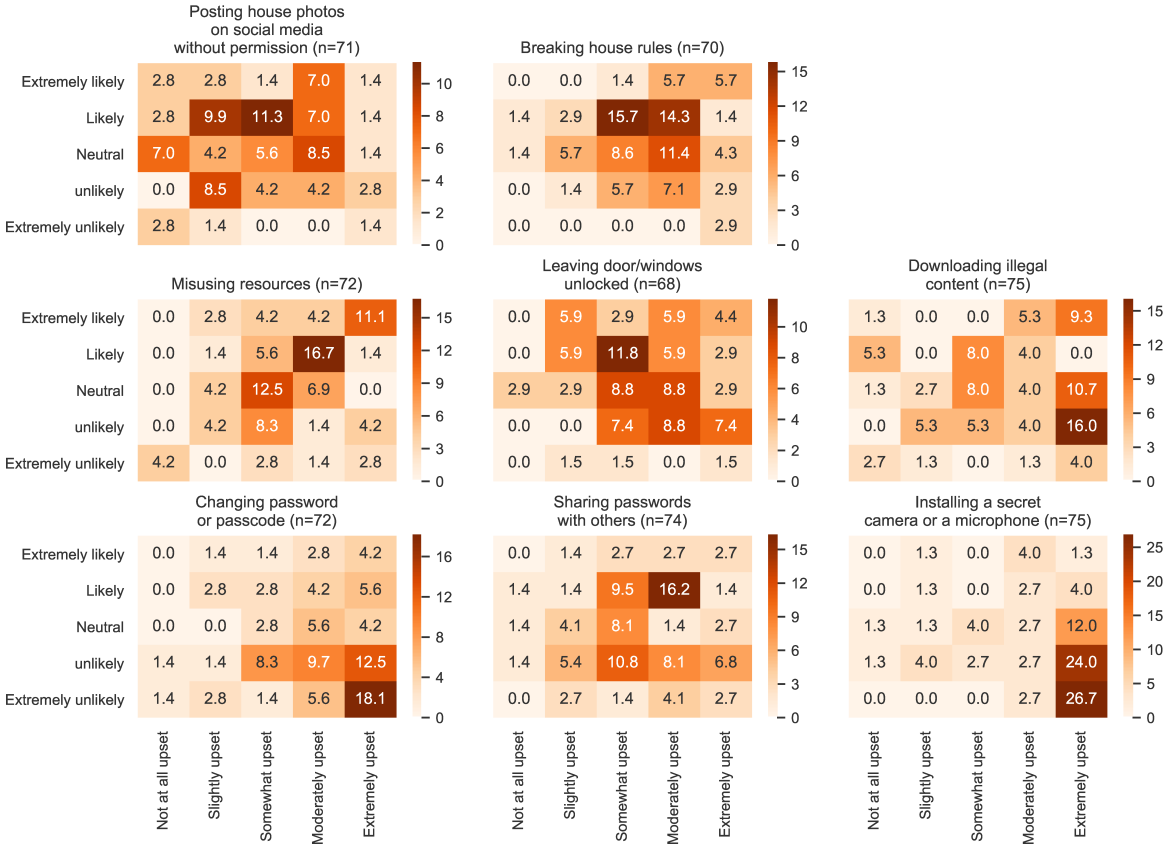

Fig. 9. Each subplot shows a heatmap of hosts' likelihood and upset ratings for one incident (given in subplot title) that can occur in *their* Airbnb. Rows represent likelihood rating and columns represent upset ratings. In a subplot, the number in each cell shows the percentage of hosts who gave a likelihood rating represented by the row and upset rating represented by the column. For instance, in subplot "Breaking house rules", the value 5.7 in the top right cell indicates that 5.7% hosts rated this incident as *extremely likely* (row) and gave an upset rating of *extremely upset* (column).

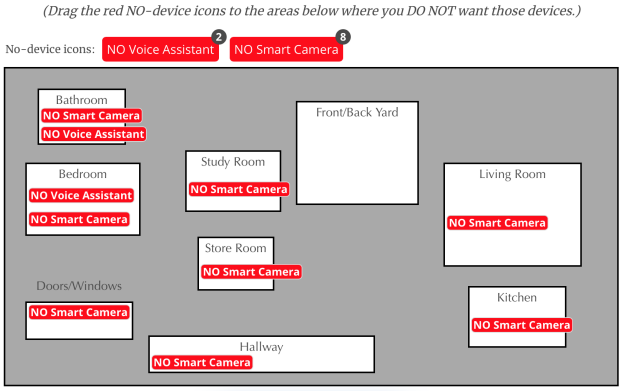

Fig. 10. Screenshot of a question in guest survey. Guests are shown devices they chose as *Depends* (shown as no-device rectangle icons on the top), and asked to indicate where in the Airbnb they do not want those smart device by dragging the no-device icons. In this figure, the devices chosen as *Depends* were voice assistant and camera.