Camille Cobb*, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer

"I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users

Abstract: Recent research and articles in popular press have raised concerns about the privacy risks that smart home devices can create for incidental users—people who encounter smart home devices that are owned, controlled, and configured by someone else. In this work, we present the results of a user-centered investigation that explores incidental users' experiences and the tensions that arise between device owners and incidental users. We conducted five focus group sessions through which we identified specific contexts in which someone might encounter other people's smart home devices and the main concerns device owners and incidental users have in such situations. We used these findings to inform the design of a survey instrument, which we deployed to a demographically representative sample of 386 adults in the United States. Through this survey, we can better understand which contexts and concerns are most bothersome and how often device owners are willing to accommodate incidental users' privacy preferences. We found some surprising trends in terms of what people are most worried about and what actions they are willing to take. For example, while participants who did not own devices themselves were often uncomfortable imagining them in their own homes, they were not as concerned about being affected by such devices in homes that they entered as part of their jobs. Participants showed interest in privacy solutions that might have a technical implementation component, but also frequently envisioned an open dialogue between incidental users and device owners to negotiate privacy accommodations.

Keywords: smart homes, internet of things, incidental users, privacy

DOI 10.2478/popets-2021-0060
Received 2021-02-28; revised 2021-06-15; accepted 2021-06-16.

1 Introduction

Smart-home devices are increasingly popular despite their demonstrated security and privacy risks. Most of the risks studied so far are relevant to the people who purchase and directly use smart-home devices, but recent studies have emphasized the importance of understanding how *incidental users*, i.e., people besides the user who owns or controls the device or service, are affected by other peoples' smart-home devices and home-automation rules [13, 44, 52] (also called *bystanders*, e.g. in [7, 52]). For example, Mare et al. found that AirBnB guests' and hosts' preferences about smart-home devices' data collection may conflict [44].

Little research has focused specifically on the risks and harms that affect incidental users. Articles in the popular press have pointed out concerning risks, e.g., of surveillance of people who work in others' homes [24] and of smart-home devices used as tools for domestic abuse [9]. A 2019 study specifically focused on bystanders' privacy perspectives about a predetermined set of situations in which participants were asked to imagine themselves as bystanders [52].

In this paper we seek to establish a ground-up understanding of the situations in which people interact with smart-home devices as incidental users and the privacy concerns and behaviors that arise. We also seek to understand the conflicts that can arise between incidental users and device owners about the deployment and use of smart-home devices and the extent to which these conflicts can be mitigated.

Specifically, we address the following questions:
RQ1: Who are incidental users? In what capacities,

***Corresponding Author: Camille Cobb:** Carnegie Mellon University, E-mail: ccobb@andrew.cmu.edu
Sruti Bhagavatula: Carnegie Mellon University, E-mail: sbhagava@andrew.cmu.edu
Kalil Anderson Garrett: Carnegie Mellon University, E-mail: kagarret@andrew.cmu.edu
Alison Hoffman: Carnegie Mellon University, E-mail: alhoffma@andrew.cmu.edu
Varun Rao: Carnegie Mellon University, E-mail: varunrao@alumni.cmu.edu
Lujo Bauer: Carnegie Mellon University, E-mail: lbauer@andrew.cmu.edu

Fig. 1. A focus group participant's drawing conveys possible privacy solutions for incidental users. A red switch at the front door is described as "use privacy switch to turn off all IoT." A person labelled "owner" is wearing a tin foil hat and announcing "we have smart devices located x, y." Another person labelled "guests" is standing next to a shelf holding more tin foil hats. A camera's presence is indicated by a marquee sign, and its range is shown with an area on the floor highlighted in orange. Text reads "until opt-in blur face." An internal door to a room with a microphone has a sign reading "For ur privacy, shut the door."

contexts, and situations are people exposed to other people's smart-home devices? Do incidental users realize when they are interacting with or exposed to other people's smart-home devices?

RQ2: To what extent are incidental users concerned about the privacy risks of smart-home devices? What (perceived) benefits and harms do they experience?

RQ3: Reacting to risks of harm (e.g., privacy concerns), what mitigation strategies do people use (e.g., avoiding walking past a neighbor's house with a Ring doorbell), and what solutions do they envision?

RQ4: In what ways are incidental users' privacy preferences aligned (or not) with those of the device owners? Or, to what extent do tensions exist between device owners and incidental users?

We explored these research questions through a mixed-methods study. We first conducted five focus group sessions (N=21) to broadly characterize the range of participants' experiences, actions, and preferences. We used the results of this study to inform the design of a survey instrument. Deploying this survey to a larger participant sample (N=386) helped us understand the prevalence of experiences and views surfaced by focus group participants, and allowed us to evaluate relationships between incidental users' preferences and factors such as situations of incidental use, types of devices, and demographic differences. Although many participants appreciated the presence of smart-home devices in a variety of situations within and outside of their own homes, they described actions they took to feel more comfortable with the devices. We find that device owners may be unwilling to accommodate incidental users or may first expect incidental users who are uncomfortable with their smart-home devices to convey specific privacy concerns that they agree are valid. Our findings highlight the importance of studying incidental users' privacy concerns and suggest that these may differ significantly from device owners' concerns. We surface tensions between device owners and incidental users, and we discuss opportunities for developing new techniques to navigate these tensions.

Key contributions of our work include:

- A ground-up understanding of situations of incidental use based on real peoples' experiences, and a corresponding quantitative exploration of the prevalence of these experiences.
- Qualitative *and* quantitative insights about incidental users' privacy concerns and the tensions between incidental users and device owners.
- Initial ideas for addressing these concerns, which are derived from users existing privacy-preserving strategies and their formative ideations.

2 Background and related work

2.1 Smart-home devices and related services

Smart-home devices are sufficiently ubiquitous that a comprehensive description is beyond the scope of this work; however, in this subsection we provide background information to help readers situate their understanding within the current state of this ecosystem.

Smart-home devices include a wide range of device types, which can react to many different types of environmental changes, and collect a variety of data. Smart speakers with voice assistants like Amazon Echo, Google Home, and Apple HomePod are especially popular. These devices typically react to a "wake word," and listen for users to ask a question or give a command. Cameras come in many forms, including security cameras for use indoors and outdoors, baby monitors, and for monitoring pets that have additional features like being able to remotely dispense a treat. Smart homes may be equipped with smart light bulbs, switches, outlets or plugs, thermostats, door locks, robot vacuums, appliances like refrigerators or laundry machines, sen-

sors (e.g., for temperature, smoke, or carbon monoxide) and many other types of devices and sensors.

Many different device manufacturers exist. Many devices have corresponding smartphone apps that let users control or monitor the devices from their phone, even when they are not at home. Devices often connect to a central hub, which may have compatibility with devices made by some other manufacturers. End-user programming services like If This Then That (IFTTT) and Samsung's SmartThings [2], allow users to create automations across various devices (i.e., including those that would not otherwise be compatible for interacting) and services (e.g., social media or cloud storage files).

There is not necessarily a clear delineation of what should count as a smart-home device, especially for the most common types of devices. For example, devices like surveillance cameras in commercial settings collect the same types of data as smart-home cameras. Voice assistants (including Amazon's Alexa and Apple's Siri) can be accessed from smart-home voice assistant devices and mobile devices like smartphones or smart watches. In some sense, when a user is at home, the privacy risks of the voice assistant on their smart watch are no different than the privacy risks of a dedicated voice assistant smart-home device. Considering these soft boundaries, it is unsurprising that users bring up mobile devices and commercial surveillance practices in the context of questions about smart homes.

It may also be ambiguous what constitutes "interacting" with a smart-home device. For example, giving a command to a voice assistant is a direct interaction, but interaction (and data collection) can also occur when a user simply enters a room and, for example, causes the temperature to rise, which may be detectable via sensors. In this paper, we take a broad definition of interaction with smart-home devices, assuming that users interact with a device any time they are near it, but this is, of course, an oversimplified definition.

2.2 Technical vulnerabilities

Like many technologies, smart-home devices are susceptible to technical vulnerabilities. These vulnerabilities have been used to turn insecure devices into actors in a large-scale distributed denial of service (DDoS) attack [27, 42]. Researchers have found that many applications built on emerging programming platforms such as Samsung's SmartThings [2] are over-privileged due to design flaws in their permission models [20, 22]. To address these types of technical vulnerabilities, researchers have proposed network-traffic-analysis-based security mechanisms [8, 15, 16, 40, 45, 46, 53], user-centric and context-aware permission systems [21, 31, 49], analyses to identify incorrect or inconsistent application behaviors [11, 38, 51], and decentralized automation platforms with more fine-grained authentication tokens [23].

Our work focuses on incidental users' perceptions of privacy risks. While these perceptions may be informed by knowledge of known vulnerabilities and high-profile attacks, the concerns that incidental users have may still arise under the assumption that such technical vulnerabilities do not exist or are unlikely.

2.3 Configuration challenges

Although smart-home devices are frequently marketed to non-technical users, prior work has identified examples of how configuration challenges can lead to security and privacy risks. Configuration challenges are especially relevant to end-user programming of smart-home devices [10, 30] (e.g., confusion about how rules will work or not realizing when their home automation programs contain bugs). Prior work suggests that users may not anticipate the security and privacy implications of their home automation rules [13, 47]. For example, Surbatovich et al. found that nearly 50% of publicly-available IFTTT rules had potential privacy leaks or integrity violations [47]. Researchers have created both static and dynamic analysis tools to help users ensure that their home automation rules work as intended and do not inadvertently lead to unsafe states [5, 12, 29, 33, 34, 39, 50, 55].

Since incidental users do not have a role in configuring smart-home devices, they may be particularly unaware of any security and privacy risks introduced by device owners' configuration mistakes. And, as with risks due to technical vulnerabilities, incidental users' concerns may persist even if device owners' configuration choices mirror what they would prefer.

2.4 User privacy preferences and incidental users' needs

Researchers have used interviews and surveys to investigate users' privacy-related experiences, concerns, and preferences [3, 4, 18, 35, 48]. Among other findings, these studies identified information that would help consumers make privacy-conscious choices when purchasing or configuring smart-home devices. Our work con-

tributes to this expanding understanding of security and privacy risks in smart-home devices by not only examining harms to users who purchase or configure smart-home devices themselves, but also to incidental users.

Most of the previously discussed literature focuses on risks that affect the person who purchased the smart-home device, or interventions that would give information to them and protect device owners from security and privacy harms. However, recent examples of smart-home-related harms to other users include devices being used in the abuse of domestic partners [9] and for spying on domestic workers [24] and neighbors [25].

When smart-home devices are installed in multi-person households, new security, privacy, and usability challenges emerge. Recent research has sought to identify user requirements in these multi-user settings and proposed potential solutions [26, 52, 54], such as designing devices to make it easier for everyone in a household to control the devices and how they are configured [54]. Others have studied desirable access controls for smart-home devices, concluding that access controls should be sensitive to factors such as the other users' relationship to the device owner (e.g., if they are a spouse, neighbor, or child) and the type of device [28, 43]. Introducing the terms *pilot* and *passenger* user to describe members of multi-user smart homes who have or have not been involved in device configuration and setup, Koshy et al. further explore these tensions between household members and ways to empower passenger users [32].

The concerns explored in these studies of multi-user smart homes include some perspectives of incidental users, but do not focus on this issue. For example, a multi-person household might consist of a married couple, their child, and an unrelated adult roommate. Both members of the couple might have mutually decided to bring smart-home devices into the home and feel equal ownership of them. On the other hand, other people living in the home, like a child or adult roommate, might fall into the category of incidental users that we focus on, if they did not have a say in the installation of the devices or do not have control of them; however, since these studies were focused on the household members, they did not identify other categories of incidental users.

Mare et al. studied AirBnBs, a specific setting in which people are frequently incidental users [44]. They found found that although guests appreciated smart-home devices, they did not always have the same views on data collection as hosts. Like our work, Yao et al. performed focus groups and co-design activities centered on incidental users (or *bystanders*) in smart homes [52]. Their study focused on three specific scenarios based on prior literature. They found that incidental users' perceptions of device utility, social relationship and trust in the device, and length of their stay in the smart home affected understanding of the situational norms, and that their knowledge about and understanding of the devices influenced their privacy-seeking behaviors. Similarly, Bernd et al. focus on privacy concerns, risks, and tensions experienced by one particular type of incidental user – nannies [7]. Our work has similarities, but contributes a ground-up understanding of incidental use of smart-home devices, starting with an exploration of what situations participants had actually encountered. We further quantify our understanding through an online survey based on our exploratory findings.

3 Methods

We used a mixed-methods approach consisting of a focus group study that informed the design of a larger-scale, demographically representative survey. Both studies were approved by our institution's IRB. The focus groups provided a ground-up understanding of the situations where people experienced being incidental users and the concerns they had, unlike related work that uses scenarios from news and prior research in specific domains [7, 52]. The focus groups also provided rich qualitative data and design insights (mentioned throughout Section 4), and they provided confidence that the survey addressed appropriate scenarios and concerns.

3.1 Formative focus group study

We first used focus groups to broadly explore people's experiences with—or as—incidental users of smart-home technology. Rather than making assumptions about the scenarios in which people encounter smart-home devices as incidental users, as well as about the risks they perceive and their compensatory behaviors, we elicited these from participants directly.

We recruited participants through local online forums (Craigslist, Reddit, Nextdoor). Recruitment materials (Appendix A) did not mention security or privacy but did show our affiliation with a security and privacy institute. Potential participants completed a screening survey to ensure that all participants had some experience with smart-home devices and that we included participants from many demographic categories. We did not aim to include a demographically representative set

of participants in these focus groups; instead we sought to elicit many perspectives to achieve a broad view of experiences that people may have with or as incidental users. Table 1 shows participant demographics. Focus groups took place in person between December 2019 and February 2020 (before COVID-19 was widespread). Each session lasted around 90 minutes, and participants received US$30 in compensation. Chronologically, the five focus groups included 5, 5, 3, 4, and 4 participants.

Focus group procedure: Participants read and signed consent forms at the start of the study and had an opportunity to ask questions before consenting. We verbally confirmed that all participants were comfortable with us audio and video recording the session, and introductions were not recorded. Each focus group session examined two main topics:
(1: RQ1&2) First, we asked participants to share examples of and reflections on their interactions with other people's smart-home devices or when someone interacted with devices they owned. Security- and privacy-related concerns were surfaced spontaneously in most sessions, even though the initial prompt was broad. When these concerns did not arise naturally, the moderator intentionally directed participants to consider these, for example by asking if there were any times when the devices made them uncomfortable.
(2: RQ3&4) Participants then split into smaller groups to discuss how the concerns and risks that came up in the session could be addressed or mitigated. We encouraged participants to draw their ideas, and provided generic pictures of smart-home devices and spaces in homes to aid the design process.

At the end of each focus group session, participants completed a brief written demographic questionnaire.

Focus group data analysis: Each session was audio and video recorded and transcribed by the first author. Following best practices for exploratory, qualitative studies, the research team reflected on our emergent findings between sessions, and the moderators incorporated this understanding in subsequent focus groups to more deeply explore key themes. After all sessions had been completed, we conducted an iterative, inductive analysis. Four authors collaborated on an affinity diagramming exercise, and we subsequently revisited the transcripts to further refine our understanding of the key themes around participants' range of concerns, situations where someone was an incidental user, and their views on possible solutions. Since the goal of the focus groups was explicitly exploratory, we do not report numerical quantities from focus groups and, instead, use them to inform our survey design and contextualize other findings. Quotes from focus group participants are attributed with a participant number that specifies which focus group session they took part in, e.g., FG2.1 is participant one from the second focus group session.

Key findings that informed survey design: Section 4 includes a more thorough description of focus group results. The following results most directly informed the design of our survey instrument. First, we used the real experiences participants described to choose five situations in which people may be incidental users and four types of smart-home devices that we incorporated into our survey (shown in Table 2). Our choices reflect situations and devices that came up most frequently and/or saw substantial variation in participants' perspectives. Second, focus groups repeatedly surfaced tensions between the expectations of incidental users and those of home owners, which we explore further in our survey. Finally, based on the potential solutions that focus group participants proposed, we produced a set of eight solution characteristics (listed in Table 4) that we asked survey participants to evaluate.

3.2 Demographically representative survey

As discussed above, our survey instrument was directly informed by the focus groups, but the survey allowed us to reach a larger and demographically representative set of participants so that we could understand how the perspectives elicited in focus groups mapped to a broader population. We included several free-response questions to give participants opportunities to surface any perspectives or experiences they had that differed from the ones we explicitly included based on the focus groups.

We used Prolific [1] to collect 400 survey responses from participants who were representative of the US population in terms of age, gender, and race/ethnicity. Survey participants were *not* required to have any experience with smart-home devices. We included two attention check questions. Participants were paid regardless of whether they answered these correctly, but we removed data from: three participants whose IDs did not match up with Prolific; six participants who failed *both* attention checks; and five of the 28 participants who failed one attention check and for whom a manual analysis of responses suggested they may not have understood survey questions or paid sufficient attention to provide meaningful answers. Thus, we collected 386 valid responses, including from 23 participants who failed one attention check but gave free-response an-

	Focus groups	*Survey*
Age	18-29 (10); 30-39 (6); 40-49 (2); 50-59 (1); 60-69 (2)	18-29 (83); 30-49 (138); 50+ (162); Prefer not to answer (3)
Gender	Male (11), Female (9), Did not specify (1)	Male (184); Female (194); Non-binary (4); Gender-fluid (1); Prefer not to answer (3)
Annual household income	Less than $50k (6); $50k-$99,999 (12); Over $100k (2); Did not specify (1)	Less than $50k (127); $50K-99,999 (162); $100K-149,999 (52); $150K-199,999 (21); $200K and above (16); Prefer not to answer (8)
Education	High school (1); Some college (3); Bachelor's (8); Master's (7); Professional degree (2)	Less than a high school degree (5); High school or equivalent (39); Some college (90); Bachelor's (133); Master's (63); Professional degree (4); Associate's degree (41); Doctorate (8); Prefer not to answer (3)
Other household members	Roommates (6); Spouse (6); Children (3); Other family members (3); Pets (4); Lives alone (2); Did not specify (2)	Roommates (35); Spouse (204); Children (119); Parents (59); Extended family (25); Pets (69); Lives alone (63); Other (15); Prefer not to answer (4)
Employment status	Not collected	Full time (147); Part time (65); Self-employed (40); Unemployed (42); Retired (56); Homemaker (17); Student (38)
Race	Not collected	White (264); Black (50); Asian (32); Hispanic (25); Multi (7); Native (2), Other (2), Prefer not to answer (4)
Experience with & exposure to smart home devices	Inclusion criteria required experience with smart home devices (as an owner or incidental user)	Had purchased, installed, configured a smart home device: Yes (283); No (103) Experience as an incidental user or device owner: Both (269), incidental user only (84), device owner only (14), neither (19)

Table 1. Summary of focus group and survey participant demographics. Survey participants are approximately demographically-representative of the US population in terms of age, gender, and race/ethnicity.

swers that showed they were paying attention otherwise. The average time to complete the survey was 11 minutes (median 9 minutes). Participants were paid US$2, which is well above the minimum wage for the US and is slightly higher than Prolific's suggested rates. The demographic breakdown of participants in our final sample is shown in Table 1.

Survey procedure: The survey (Appendix B) started with participant consent and an overview of the types of smart-home devices we asked about (with pictures and examples). It concluded with demographic questions. The rest of the survey had four parts, approximately corresponding to our research questions:

(1: RQ1) To help us understand the prevalence of incidental users' experiences, participants indicated which of four types of devices they had seen in each of five situations (Table 3). Participants could optionally describe other situations in which they had seen smart-home devices.

(2: RQ2) We next explored participants' level of privacy concern vs. perception of device utility (i.e., their *appreciation* of the devices). Participants were shown a block of questions related to each situation type. These five blocks appeared in a randomized order, and we did not account for any ordering effects in our analysis. For each block, participants answered the following prompt on a seven-point scale from "strongly dislike" to "strongly appreciate": *Considering the privacy impacts and utility benefits of each type of smart home device in [situation type], how much do you appreciate or dislike having this device around?* When participants had previously indicated that they had not seen any devices in this situation or that the situation did not apply to them at all, the question phrasing was adjusted to reflect this and emphasize that they should answer how they believe they would feel. Without referring to any particular type of device, we then invited participants to specify in a free-response field: *If you have taken any steps to make yourself feel more comfortable about smart home devices at [situation type], please describe what you did.*

(3: RQ4) In the question block about participants' experiences in their own homes, there were several additional questions. First, considering the types of devices that participants *had* seen in their own homes, we asked which ones they owned; comparing this against whether they had seen a device in their home gave us a lower bound on the number of participants who had been incidental users in this situation. Then, after asking them to indicate their appreciation or dislike (as above) and what actions they had taken, we asked if they would be willing to turn off smart-home devices or move them to another location if they found out they were mak-

ing others uncomfortable. Specifically, this included four questions, randomly ordered, asking if they would do so for *your neighbors*, *someone else you live with*, *a friend or family member who is visiting your home*, or *someone working at your home (e.g., package delivery person or babysitter)*. Participants could answer "yes," "no," or "it depends," and if they chose the latter, they could use a free-response field to describe what factors would influence their choice. This allowed us to further examine the tensions that may arise with device owners when incidental users have privacy concerns.

(4: RQ3) Finally, we asked participants to *Imagine a situation in which a smart home device that someone else owns causes you to feel uncomfortable about your privacy (i.e., because the device could collect data about you)* and rank eight characteristics that a solution should have in order to make them feel more comfortable. They could sort the characteristics into three bins, depending on whether the characteristic was *very important*, *somewhat important*, or *not important* to them. We also invited participants to write in any other characteristics they felt a solution should or should not have.

Statistical analyses: We first performed statistical analyses to examine the relationship between demographic and situational factors and participants' appreciation of devices (i.e., responses from (2) in the above survey procedure, measured via a seven-point scale) in the 20 scenarios (i.e., 4 device types x 5 situations). We mapped each seven-point Likert scale response to a binary variable with values 0 and 1, where 0 implies a negative preference and 1 a positive preference. We included neutral responses in the positive preference bucket so that we could separate users who are *un*comfortable from everyone else, as these users in particular may need better privacy solutions. Precedent exists for dichotomizing Likert responses such that statistical insights align with research questions [14, 19, 41], and we additionally report the number of participants who indicated each response value in Figure 2. We considered this binary variable as our outcome. The factors we studied in relation to this outcome included situation type, device type, whether the participant actually encountered the scenario, if they were a device owner or incidental user, and demographics. The survey generated repeated-measures data; hence, we modeled the relationship between factors and the outcome describing appreciation using generalized linear mixed model (GLMM) regression [6].

We also studied how a participant's general appreciation of smart-home devices in different scenarios, along with whether they are device owners and their demographics, are related to willingness to accommodate others. Participants indicated willingness to accommodate four different groups (i.e., responses from (3) in the study procedure). As with the Likert-scale responses, we report the number of participants who chose each option (see Table 5). Although participants could respond with "yes," "no," or "it depends," for statistical analyses we mapped these responses into binary outcomes of "yes" and "no." "It depends" was bucketed with "yes" to distinguish people who would not consider accommodating others from those who would (at least) sometimes. The yes/no answers to these four questions were the outcomes. The factors we studied in relation to these outcomes included how many times a participant indicated a positive appreciation for a smart-home device out of the 20 scenarios they were asked, whether the participant was a device owner or incidental user, and their demographics. We built four logistic regression models to study what factors are correlated with each of the four outcomes after ensuring the assumptions of the models were met, which involved removing colinear variables.

Tables showing the results of all models are included in Appendix C.

Analysis of free-response answers: For free-response answers where participants described actions they had taken in a particular situation to feel more comfortable about smart-home devices and what factors affected that their willingness to accommodate incidental users' privacy concerns, we performed additional qualitative analysis. Two researchers independently performed an inductive thematic analysis of responses, met

Device type	***Shorthand***
Smart or Internet-connected cameras	Cameras
Voice assistants	Voice assistants
Smart lights, thermostats, plugs, or door locks	Lights, thermostats, etc.
Smart appliances and other types of smart home devices	Other types of smart devices
Situation	***Shorthand***
At your own home	Home
At a friend or family member's home	Friend's home
At a neighbor's home	Neighbor's home
At a short term rental (e.g., Airbnb)	Rental
While you were at someone else's home for work	Work

Table 2. Our survey included questions about four types of smart home devices and five situations that might involve incidental use of these. Inline descriptions sometimes use shorthand for these.

to reach consensus about the themes identified, and independently applied the codes to the data. We reached consensus by discussing disagreements, which were very few. The structure of this analysis and consensus building aligns with previous work [37]. Though we report the number of responses that fit each theme, these questions were optional and open-ended; therefore, some participants who did not answer, or whose answer did not fit a particular code, would likely have agreed with the ideas that other participants put forth. For this reason, we do not make statistical claims based on these answers. Quotes from survey respondents are attributed to randomly-assigned participant IDs from S1 to S386.

4 Results

4.1 RQ1: Characterizing incidental users and situations of incidental use

Understanding the range of situations in which someone might become an incidental user is needed to develop a holistic understanding of user experiences and concerns. Prior work and popular press have surfaced specific risks, but our work provides broad insight based on participants' experiences.

When do people become incidental users? In focus groups, participants described a wide range of situations in which they had encountered someone else's smart-home devices or in which other people came into or near their smart-home devices. Additionally, although we asked about five specific situations in our survey, several participants wrote in free-response answers that described other situations of potential incidental use.

Dimensions along which these situations varied included the relationship (and trust) between the device owner and the incidental user (e.g., family members, friends, or people with less close relationships) and the circumstances that brought the incidental user into the vicinity of another person's devices (e.g., living with or near them, social visits, or work-related reasons to be there). For example, FG1.2 stayed at her sister's house for a few weeks, where there were smart cameras and voice assistants, and FG5.1 lived with roommates who had a Google Nest in the shared living room. Survey responses suggest that it is common for roommates to become incidental users in their own home: of the 35 survey participants with roommates, 23% had encountered devices in their home that they did not own, compared to only 12% of all 386 participants.

Focus group participants also conveyed that factors such as the length and frequency of time they spent in a place, whether they went inside, and whether the homeowner was there with them were potentially important. These dimensions and factors are not independent of one another. For example, encountering a device in a short-term rental would typically involve being inside (not just outside), stays that last overnight, the device/home owners not being present, and a financial rather than social relationship between the device/home owner and the renter. Some of these situations also do not apply to everyone. 16% of participants reported that they do not have neighbors, only 32% of participants' indicated they go into other people's homes for work, and 57% said they had not stayed at a short-term rental (recently). Focus group participants gave several examples of jobs or professions that would frequently involve being at another person's home (where there might be smart-home devices), and the occupations of survey participants with this kind of incidental user experience provide additional examples. These may include: pet-, baby-, or house-sitters, delivery couriers, (home) health caregivers, laborers, educators (e.g., for tutoring), pest control professionals, and firefighters.

In both the focus groups and survey free-response answers, participants mentioned seeing surveillance devices that are similar to smart-home devices (e.g., security cameras) in stores or other public places, not just homes, and some survey participants described seeing commodity smart-home devices (e.g., Amazon Echo) in small businesses. Thus, it may be possible to be an incidental user of smart-home devices outside of a home environment, which was beyond the scope of our study.

What devices do people notice as incidental users? Focus group participants brought up many different types of smart-home devices, sometimes conveying thoughts about the utility or privacy risks associated with a particular manufacturer or type of device (e.g., related to the type of data it could collect). Experiences with cameras and voice assistants typically drew the most discussion in focus groups. The discussion moderator sometimes needed to initiate or encouraged further discussion of other types of devices, like smart lights, thermostats, plugs, door locks, smart appliances or robot vacuums, though many participants did have direct experience with these types of devices.

Focus group results suggest that incidental users may not always notice a smart-home device or recog-

nize it as such. For example, some participants, like S324, may miss devices because they are not actively looking for them: *"I never really notice or pay attention."* FG3.3 pointed out the difficulty of being confident in their knowledge of what devices are (or are not) around: *"I think it's kind of hard, especially if the devices are hidden."* In some cases, incidental users might realize that a device is present but not understand how it works and how it might affect their privacy, as in FG1.1's experience: *"the head of the household, he has this weird device. I don't even know what it is but there's sensors around the whole house."*

Prevalence of experiences as incidental users. Table 3 shows how many survey participants reported seeing each type of device in each situation. Responses indicate that 353 participants (91%) had been incidental users in some situation for some device, and for each type of device we asked about, at least half of participants had said they had encountered it as an incidental user. Our survey did not explicitly ask if participants were incidental users in their own home, but 45 participants (12%) reported seeing some type of devices in their home that they did not own themselves. 63% of the participants who *do* go into other people's homes for work had seen a device there.

4.2 RQ2: Perceived device utility and (privacy) drawbacks

Although users might not always anticipate the possible risks associated with smart-home devices, understanding what concerns they do have—and what tradeoffs or other factors may influence them to accept these risks—can guide researchers and designers to solutions that address relevant issues. Since we prompted focus group participants to reflect broadly on their experiences with devices in other people's homes, the discussions included topics beyond just the security and privacy risks to incidental users. They described security and privacy concerns from the perspective of incidental users *and* device owners and other aspects of smart-home devices that they disliked or appreciated.

Beneficial uses of smart-home devices. Discussion of risks was situated within participants' beliefs about the beneficial uses of smart-home devices—including potential benefits to incidental users. For example, FG1.3 explained that *"Someone stole a bike from my backyard. I discovered my neighbor had a camera that had been pointed at me."* FG1.2 pushed back: *"I don't know if that [camera placement]'s legal,"* but FG1.3 countered *"Well, it turned out great because we got the bike thief!"* In addition to home security, participants also described enjoying devices for their convenience and entertainment.

Device owners' concerns about incidental users. Participants in several focus groups described worrying about incidental users' interactions with their devices. For example, they noted that guests could ask their voice assistant to describe recent purchases (which might be sensitive or private) or could play music through paid services (e.g., Spotify) that they feared would automatically charge them. Similarly, FG3.3 worried that by playing music on her friend's smart speaker, she would mess up the device's understanding of the owner's music tastes. FG1.2 cited a reason besides privacy for disliking devices' presence when guests were around: *"I sometimes turn it off when other people come over, because I don't really want them to spend time using it. My [family] like it, so they spend a lot of time [with the device] and they don't talk to me.* The focus of our study was on privacy risks that apply *to* incidental users, but these additional concerns may contribute to tensions or reveal opportunities for alignment between incidental users' and device owners.

Incidental users' privacy concerns. Thinking of times when they had been incidental users, focus group participants mostly described a general sense of unease rather than specific privacy concerns. For example, FG1.5 *"used to be a delivery driver, and I'd see [home surveillance cameras] all the time. I even had a couple of customers tell me can you look up to the left or can you look up to the right. So they can see my face."* He said that this made him feel *"kind of creeped out."* Participants' concerns pertained to device owners or other people, governments, advertisers, and device manufacturers. Discussion suggested that the level of concern varies depending on the type of device, its specific location (e.g,, FG3.1 said *"but what if it's in the bathroom, what if it's somewhere you have an expectation of privacy?"*), their closeness with and trust of device owners, how often or how long they are at the home, and more.

Other incidental user concerns and frustrations. Another interaction that came up repeatedly was the use of devices to harass or tease. For example, FG1.2 described using smart speakers to play music that the device owner would not like, and FG1.1 brought up a use that they would see as unacceptable: "what i worry about the bathroom lights is if my roommate messes with me saying like 'turn off the bathroom lights' when i'm in the shower." For FG1.3, smart lights in their bath-

% (count) of participants who ...	... had encountered some type of device	... had not encountered any type of device	... this situation does not apply to them	... had encountered a **camera**	... had encountered a **voice assistant**	... had encountered **lights, thermostats, etc.**	... had encountered **appliances or other smart home devices**
Experiences including all situations	96% (369)	4% (17)	N/A	72% (278)	88% (341)	70% (271)	58% (222)
Experiences as an incidental user including all situations	91% (353)	9% (33)	N/A	67% (259)	81% (313)	61% (236)	53% (204)
At their own home (all)	83% (320)	17% (66)	N/A	35% (135)	63% (244)	41% (159)	27% (105)
At their own home (encountered devices they do not own)	12% (45)	N/A	N/A	4% (16)	4% (15)	3% (10)	3% (13)
At a friend or family member's home	80% (309)	20% (77)	N/A	57% (221)	77% (298)	53% (203)	46% (176)
At a neighbor's home	53% (206)	31% (119)	16% (61)	38% (146)	34% (133)	26% (100)	19% (72)
While at someone else's home for work	20% (77)	12% (45)	68% (264)	13% (49)	16% (60)	11% (44)	8% (32)
At a short-term rental	28% (109)	15% (59)	56% (218)	13% (50)	13% (49)	19% (74)	12% (46)

Table 3. Device encounters across situations and device types. For example, 259 participants said they had encountered a voice assistant in a friend or family member's home. 61 participants said they do not live close enough to anyone to consider them a neighbor, 264 said they do not go into other people's homes for work, and 218 said they have not (recently) stayed in a short-term rental.

room were once accidentally turned off while an incidental user was inside; when this happened, the incidental user texted them to correct the mistake.

Additionally, some participants focused on reasons besides privacy that led them to dislike smart-home devices, such as feeling that new-to-them voice assistants (i.e., at a house they were visiting) needed time to learn to understand them, or discussing the problem of entering a smart home and not knowing how to do basic things like turn on the lights.

Privacy-utility tradeoffs for specific devices and situations. Focus group participants' positioning of privacy risks within the context of other benefits informed our choice to explicitly frame our survey questions in terms of this tradeoff. We asked participants how much they appreciated or disliked having a particular type of device around in a particular situation. Responses are summarized in Figure 2.

Across all situations and device types, survey participants reported feeling mostly positively about the privacy-utility tradeoffs created by smart-home devices. Out of 7,704 responses about comfort with a particular device in a particular situation, they reported disliking its presence only 20% of the time, and were only *strongly disliking* it 9% of the time, compared to feeling somewhat to very appreciative of devices in nearly 50% of cases and neutral in over 30% of cases.

We also studied what factors affect how comfortable people feel in the presence of smart-home devices. Our results show that the type of device, the particular situation under consideration, whether the participant had smart-home devices, and whether they had actually experienced this situation had a statistically significant correlation with participants' rating of their appreciation or dislike. Demographics including age, race, binary gender, and household income were not significantly related to how participants rated their appreciation or dislike of smart-home devices.

Relative to the baseline of encountering smart-home devices at their own house (which most participants rated as leaning toward appreciating rather than disliking), participants were even more likely to view positively devices in their neighbor's house (coef = 1.040, $p < 0.001$) and at work (coef = 0.366, $p = 0.007$); however, the opposite was true for devices at a short term rental, where participants were significantly more likely to dislike the devices' presence (coef = -1.190, $p < 0.001$). For the scenarios we asked about, devices in participants' own homes were reported as arousing concerns 17% of the time; while devices in short-term rentals aroused concerns 33% of the time. In terms of different types of devices, we used appliances and other types of smart-home devices as the baseline, and found that participants were more likely to dislike cameras (coef = -3.116, $p < 0.001$) and voice assistant devices (coef = -2.183, $p < 0.001$), but their views on lights, thermostats, etc. were not significantly different from the baseline. In particular, 25% and 36% of responses conveyed privacy concern about cameras and voice assistants, respectively, compared to only 11% for appliances. Additionally, participants who owned (i.e., had purchased, installed, or configured) a smart-home device themselves were more likely to be appreciative of the presence of all types of devices in every situation. In particular, we included a feature describing whether a participant had been a device owner, an incidental user, both, or neither. Considering the baseline to be a participant being both, participants were less likely to appreciate smart-home

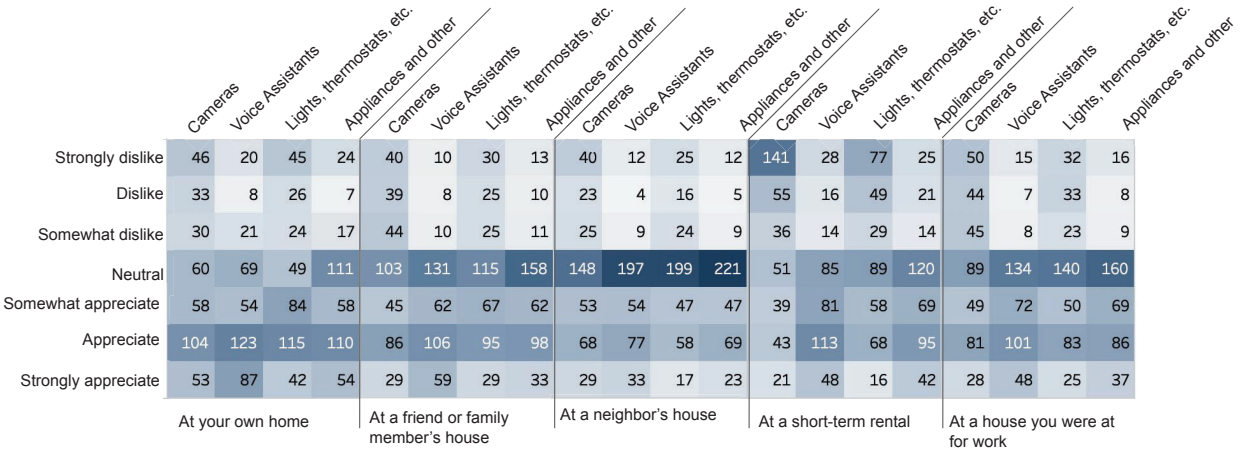

Fig. 2. Heatmap of Likert scale responses conveying participants' evaluation of the privacy risk vs. utility tradeoff for each device type and situation (each survey participant responded for all combinations of device and situation).

devices if they were not device owners (incidental user only: p = -2.164, p <0.001; neither: coef = -2.043, p = 0.001). Participants who had been both (baseline), across all situations and device types, were concerned in 21% of responses; while participants who were only incidental users, or neither, were concerned in 26% and 42% of responses, respectively.

These analyses include responses from all participants—including those who had *actually* been an incidental user in a particular context (i.e., situation and device type) and those who were *imagining* how they would feel if they encountered a particular device in this situation (including if the situation, such as being in someone else's house for work, did not apply to their life). We found that participants who had actually seen a particular type of device in a particular situation exhibited a higher likelihood to appreciate the presence of that device in that situation (87% of responses were appreciative or neutral) compared to participants who were imagining how they would feel (76% of responses were appreciative or neutral; coef = 0.940, p <0.001). Appendix C includes the results produced by the regression model.

4.3 RQ3: Reactions to and desired solutions for privacy risks

Mitigation strategies participants had used. In describing their experiences with smart-home devices, focus group participants frequently spontaneously volunteered information about actions they had taken to feel more comfortable about the presence of these devices, or to avoid having them around. For example, FG1.4 lived with unrelated roommates and said: *"when people were looking at my house, I wrote it into the lease that they were not allowed to bring voice-activated anything in."* Many survey participants also wrote-in meaningful free-response answers about the actions they had taken to feel more comfortable about smart-home devices in each of the five situations, which closely mirrored the actions described in focus groups.

Fifty four participants described taking a direct action, including unplugging, muting, and covering devices, which would disable the device or otherwise prevent data collection. Sometimes they described taking these direct actions preemptively to avoid a general discomfort, or situationally if they believed they would not need or want to use the devices for beneficial purposes, or at times when they felt especially privacy-conscious (e.g., to have a sensitive conversation).

Thirty participants said that they had changed their behavior (e.g. by avoiding devices, moving locations of conversations, and shortening stays) to avoid having embarrassing, private, or compromising data collected about them. For example, S204 wrote *"For the devices in other places, I try to make sure I do not look like I am in a compromising situation or I am performing an action that can be seen as something else. I try to be clear with what I am doing and limit what I say. For the part of what I say, it it is to keep info to being ambiguous or general and it does not reveal info that I would not want any one else to know."*

Twenty five participants wrote that they learned more about how the devices work in order to feel more comfortable. They did not always specify their goals of

this information-seeking, but some participants seemed to be learning how to get the full beneficial utility from the device, whereas others were trying to better understand the privacy risks.

In focus groups, participants frequently proposed mitigation strategies that would involve a conversation and negotiation between the device owner and a privacy-concerned incidental user, but only 6 survey participants said that they had taken this kind of action. For example, FG2.1 mentioned that as a device owner, *"sometimes people will say stuff about [my voice assistant], and sometimes I have to unplug it"*. FG3.2 imagined that as an incidental user they *"would ask [the device owner] about [their smart camera]. Why would [the device owner] measure the bathroom, I mean?"*, and FG3.1 agreed, saying *"I would too"*.

For devices in their own homes, participants noted taking actions like securing their home network to minimize the risks of technical vulnerabilities, limiting the types of devices installed in the home or choosing a location for the devices with privacy in mind (e.g., being willing to only have cameras outside of the home, not inside), or (like FG1.4) avoiding the devices altogether *"What I do to make myself feel more comfortable is not buy that datamining trash :)"* (S110). Although these responses to free-response questions should not be interpreted as generalizable insights, the differences in mitigation strategies used each situation supports the idea that incidental users may be limited in what actions they can take or feel comfortable taking. For example, 33 participants described taking direct actions in their own home but only 6 said they did so at a friend or family member's house. This idea is also supported by the 43 participants who said they would not take any action to make themselves feel more comfortable about other people's devices; although some of these responses indicate that the lack of action is due to not feeling uncomfortable, several participants said they would simply *"try to forget [the devices] are there"* (S279); S254 explained *"If I am at a friends or family member's house it is not for me to decide what they use or how, so I just live with their decision."* Often, participants just wanted to be informed about the presence of devices, like S114: *"I do not care either way about what smart devices my friends and family have in their home, provided they inform me beforehand."*

Privacy solutions envisioned by participants. The second portion of our focus group procedure focused on envisioning possible solutions to the privacy risks and other challenges with smart-home devices that they had previously identified. Participants' proposed solutions included technical, legal, and/or behavioral changes. Some of these actions and proposed solutions were more readily achievable (either by incidental users themselves, or by device designers without requiring novel technical innovations), whereas others were unsolved and varied in terms of how realistic they would be to implement. Some survey participants also wrote in specific ideas for more privacy-preserving device designs when we asked them what characteristics they thought solutions should have. While we surface examples of the proposed solutions here, they are not exhaustive of what participants suggested.

Fig. 3. Voice assistant announces "You may be getting recorded."

Fig. 4. Drawing from focus group session 4. Shows an image captured by a camera device where a person's face is obscured. Text reads "software makes data it keeps anonymous."

Some proposed solutions came up repeatedly. For example, many participants envisioned physical signs, like those used to indicate that someone has a traditional home surveillance system, that would warn incidental users if smart-home devices were present (illustrated in Figures 1 and 6 from the focus groups). Similarly, other suggestions conceived of devices that would audibly notify nearby incidental users of their presence, either with voice (as in Figure 3 or with more subtle sounds like beeping). Both focus group and survey participants suggested a modified voice assistant that could identify who was speaking so that it could ignore or se-

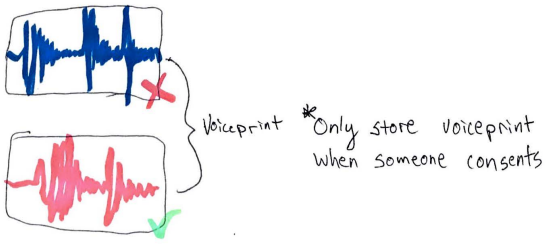

Fig. 5. Drawing from focus group session 5 that shows two audio signal graphs. The top one has a red X, and the bottom has a green check next to it. Text next to the figure reads "Voiceprint—only store voiceprint when someone consents."

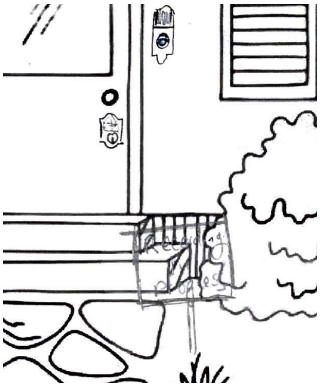

Fig. 6. Focus group participant added to a drawing of a front door. They show a smart door lock and Ring doorbell, but also a sign in the yard that reads "Recording in progress."

lectively delete (not save) data from individuals who preferred privacy or had not consented to data collection. S65 described this idea and the potential limits of its privacy benefits: *"Go ahead and record my voice once, then if you pick it up don't use it further. With AI though this is ridiculous b/c a conversation could still be understood through context and the other person!!"* Figure 5 shows a visual rendition of this from the fifth focus group session. Other proposed technical solutions included anonymizing (e.g., blurring) identifying data about incidental users (illustrated in Figures 1 and 4).

In addition to yard signs that would need to be installed by device owners, other behavioral solutions were also proposed, some which would require effort on the part of device owners and others that would rely on privacy-conscious incidental users being proactive. Figure 7 shows a device owner proactively informing incidental users about the presence of smart-home devices *and* an incidental user checking to see if there are voice assistant devices that could be listening.

Evaluating solution characteristics We distilled solutions proposed in focus groups into high-level goals

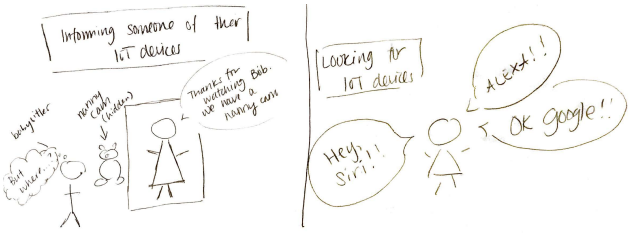

Fig. 7. Drawing from focus group participant with two parts. Left side shows a device owner warning someone about devices. Right side shows an incidental user actively checking for voice assistant devices by saying the most common wake words.

or characteristics that incidental users (or device owners) might want the solution to have. We asked survey participants to imagine a situation in which a "smart home device that someone else owns causes you to feel uncomfortable about your privacy," and to indicate whether each of these characteristics was very important, somewhat important, or did not matter to them. Participant responses are summarized in Table 4.

Four solutions stood out as being "very important" to at least 70% of participants, and every solution was marked as "very important" to over 20% of participants. A plurality of participants rated the characteristic *Conform to social conventions* as unimportant to them, which may be consistent with the proposals for privacy-preserving solutions that would involve asking device owners to make adjustments to their smart-home setup and with responses that expect privacy-concerned incidental users to explain their concern. Additionally, almost half of participants rated *Require minimal effort from the device owner* as unimportant, which may be because our survey posed this question from the perspective of incidental users (i.e., rather than device owners). This result points to potential discrepancies between device owners' and incidental users' priorities.

4.4 RQ4: Device owners' willingness to accommodate incidental users' privacy preferences

When asked if they would be willing to turn off or relocate smart-home devices that made incidental users uncomfortable (Table 5), 41 participants (10%) reported that they would not be willing to accommodate *any* of these other people, and only 80 (21%) said that they would be willing to make these accommodations for all of these other people. That is, 69% of participants would be willing to make accommodations for some incidental

	Very important	Somewhat important	Do not care	Not ranked
Let me know what data nearby devices will actually collect	**73% (282)**	17% (66)	6% (24)	4% (14)
Let me know when nearby devices are currently collecting data	**73% (282)**	18% (71)	5% (19)	4% (14)
Give me a chance to avoid data collection	**73% (280)**	16% (60)	9% (33)	3% (13)
Let me know when a device is present	**70% (271)**	19% (73)	6% (25)	4% (17)
Let me know what type of data nearby devices are capable of collecting	**65% (251)**	26% (100)	6% (24)	3% (11)
Let me know exactly where a device is located	**55% (214)**	29% (113)	11% (44)	4% (15)
Require minimal effort from me	**42% (161)**	32% (123)	21% (81)	5% (21)
Give me a chance to adapt my behavior	29% (111)	**37% (141)**	31% (118)	4% (16)
Require minimal effort from the device owner	26% (100)	24% (93)	**46% (176)**	4% (17)
Conform to social conventions (e.g., not require anyone to do something that would be seen as rude)	23% (87)	34% (130)	**40% (154)**	4% (15)

Table 4. Considering eight possible characteristics of solutions to privacy concerns about other people's smart home devices, participants specified whether the solution was "very important" or "somewhat important" to them, or if they did not care about it.

Person	Yes	No	It depends
Your neighbors	29% (111)	**55% (211)**	16% (62)
Someone else you live with	**76% (295)**	15% (58)	9% (33)
A friend or family member who is visiting	**65% (250)**	26% (100)	9% (33)
Someone working at your home	36% (139)	**52% (200)**	12% (45)

Table 5. A summary of participants' responses to "Would you be willing to turn off or move devices if you found out they were making [person] uncomfortable?"

users but not others or would only do so dependent on other factors, which they specified in writing.

When participants indicated "it depends" and wrote-in answers, they most frequently specified that they wanted to evaluate the reason for the other person's discomfort (37 unique participants and 51 of the 162 write-in answers, considering all four types of incidental users we asked about). For example, S347 said *"I would have to evaluate their objections."* Giving more details about what responses are (or are not) acceptable, S120 stated that *"It depends [on] what the reason was. My cousin who's paranoid about big brother listening in, no we would not turn it off. perhaps if it were a cultural issue for someone, I'm open to turning them off."* Across 47 write-in responses, 38 unique participants said their choice would depend on their relationship or trust of the person who was uncomfortable. However, in some cases this may be a self-defeating proposition, since, as FG2.4 worried *"you become suspicious just by you voicing your privacy concerns."* 23 participants (31 responses) said that their willingness to make these accommodations hinged on this not infringing on their own utility from the device (e.g., not compromising the added home security their devices provide), and in 19 people they said they would assess the validity of their discomfort (independently of reasons given by the incidental user). For example, S368 stated that they would accommodate their neighbor *"If I can determine it is invading their privacy or intefering [sic] with their life style."*

In all four logistic regression models related to participants' willingness to turn off or relocate smart-home devices if they found out that they made others uncomfortable (see Tables 7–10), participants who were generally more comfortable with smart-home devices (i.e., participants who reported feeling appreciative or neutral about a greater number of scenarios than others) were less likely to accommodate others. In particular, for each additional scenario for which they indicated appreciation (between zero and 20 scenarios), participants were approximately 0.98× as likely to be willing to accommodate a neighbor, housemate, friend, or worker in their own homes ($p < 0.001$). For example, people who indicated appreciation for all twenty scenarios would be only 0.667× as likely to indicate willingness to accommodate as people who indicated appreciation for none.

No other factors (including owning a device or having been an incidental user, gender, age, or income) were correlated with a higher or lower willingness to accommodate except for the outcome describing willingness to accommodate workers. In this case, older participants were less likely to accommodate workers in their homes. Specifically, compared to the baseline age group of 18-29, participants in the age group 30-49 were 0.82× as likely to turn off or relocate smart-home devices and participants in the 50+ age group were 0.77× as likely. The results of these models are in Appendix C.

5 Discussion

5.1 Incidental use situations & prevalence

Many people are incidental users. Our study shows that almost everyone at least sometimes experiences being an incidental user (over 90% of survey participants). Device ownership is also widespread (nearly 3/4 of survey participants had purchased, installed, or configured a smart-home device). Thus, it is important and relevant to understand and address incidental users' privacy preferences alongside device owners' smart-home goals. Although manufacturers may want to appeal primarily to (potential) device owners, rather than incidental users, several focus group participants described initially encountering a new type of device as incidental users and wanting one for their own home.

We found similar situations of incidental use to prior work. The situations of incidental use we identified aligned with those considered previously. For example, our short-term rental situation closely matches Mare et al.'s focus on AirBnBs [44] and Yao et al.'s temporary residency scenario [52], and concerns related to neighbors and employment have been discussed in news articles [24, 25]. Participants also mentioned situations we had not considered. They had seen commodity smart-home devices (e.g., Amazon Echo) in businesses and friends' vehicles, blurring the lines of where smart homes end and the distinction between smart-home devices and traditional surveillance in public places. They also noted that mobile devices may carry the same or similar capabilities (in particular, voice assistants) as smart-home devices. These findings relied on participants recalling and self-reporting when they had seen devices; there may be additional situations of incidental use that were not considered in our work. For example, researchers noted the possibility of being an incidental user through video calls (e.g., triggering voice assistants), though no participants mentioned this context.

Prevalence of privacy concerns. Although most participants were appreciative of or neutral toward devices across all situations and device types, it was not unusual for someone to dislike a device (20% of the time participants expressed negative feelings about devices). We also find that a small but not insignificant population encounters smart-home devices as incidental users despite not owning them (8.5% of survey participants). Furthermore, despite being representative of the US census, our survey likely still disproportionately reached people who were more likely to own smart-home devices (e.g., people experiencing homelessness would likely not own smart-home devices but might still be incidental users), and so this may represent a lower bound on the gap between device owners and incidental users.

People whose preferences and needs have not yet been considered. The population of incidental users who are not device owners is especially important for several reasons. First, prior work studying privacy concerns and risks related to smart homes has predominantly focused on device owners, so little is known about other stakeholders' perspectives. Our finding—that people who own devices tend to also appreciate them more (i.e., lean less toward disliking them due to their privacy risks)—suggests that people who do not own smart-home devices may think very differently and have different preferences than device owners. Encouragingly, participants who had actually experienced interacting with a particular device as incidental users rated their appreciation of it higher than those who were just imagining how they would feel. This may indicate that people tend to overestimate their privacy concern and acclimate to the presence of devices with experience. It could also suggest that some privacy-conscious individuals successfully avoid undesirable situations of incidental use (a choice that may not be available to all, especially for people whose work requires them to regularly enter other peoples' homes).

5.2 Tensions with device owners

Internal tension about what is appropriate. In focus groups especially, many participants described feeling strongly that they should not be surveilled without giving consent (e.g., S110 wrote *"Sick of how we think 'consent' means 'I'm going to describe what I want to do to you, and then I'm going to do it, you have no choice.' . . . Opt-in only!! Treat data collection like it's sex. It's about as intimate"*). However, many participants also felt strongly that they—and others—should have the right to set up whatever devices and data collection they desire in or at their own home. These beliefs sometimes co-existed within the same person even when they acknowledged that the views were contradictory.

Device owners are often willing to accommodate incidental users, but tensions remain. We were surprised to find that so many participants (envisioning themselves as device owners) *were* willing to accommodate incidental users if they had privacy concerns,

particularly for visiting friends and family members or people they lived with. A significant portion were willing to accommodate neighbors and people working at their home, whom they may not know as well. Of course, our question phrasing *assumes* that the device owner would find out about incidental users' concerns, which may not occur in practice. This means that someone who is especially concerned about their privacy may be able to meet their privacy needs through conversations with device owners, but this may not always be practical or effective. For example, delivery couriers likely encounter devices (e.g., security cameras) at many different homes per day; not only is it likely that device owners would not be home or that the incidental user would not have time to converse, but they are certain to encounter some device owners who would be unwilling to accommodate their privacy preferences even if they could have this conversation. Many participants also said they expected to hear a well-substantiated argument about why a device seemed privacy-invasive before accommodating concerns, even though focus group participants more often expressed a general unease rather than clear reasons for concern.

5.3 Meeting incidental users' needs

Our findings point to promising future directions to address tensions between device owners and incidental users. It may be especially important to create privacy-focused solutions for the most common situations of incidental use (e.g., 80% of survey participants were incidental users when visiting a friend or family member's home) or the situations in which users are especially likely to be worried about their privacy (e.g., statistical analysis indicated greater concern in short term rentals than other situations). However, as argued by McDonald and Forte [36], rather than prioritizing solutions based only on these norm-based metrics, solutions should also prioritize incidental users who are most vulnerable, even if they are not the majority.

Create tools for conveying devices' presence and functions. Participants frequently expressed a desire to at least be informed about the presence of smart-home devices, even if they could not (or would not ask for) data collection to be turned off. Being aware of the devices' presence is also a necessary precursor to adapting one's behavior because of the device (e.g., avoiding sensitive topics or leaving an area altogether, as some participants described doing). While some participants suggested that device owners should go out of their way to inform others about devices (as in the solutions illustrated in Figures 1, 6, and 7), this could also be accomplished through technical means, for example sending smartphone notifications when devices are nearby. Existing recommendations for conveying the privacy risks of devices (e.g., [17]) are predominantly aimed at people considering purchasing one. Designers should consider how to convey relevant details to incidental users about the devices and their configuration, such as what data will be collected or the area captured by a camera.

Make it easier for incidental users and device owners to communicate. Since we found that many device owners would be willing to accommodate incidental users if they learned about their privacy concerns, we suggest investigating mechanisms for encouraging conversations. The tools proposed previously that would inform incidental users might also spur conversation. Discussion may also benefit from scaffolding; for example, device owners may want to explain their reasons for having certain devices, and incidental users might appreciate help explaining their privacy concerns. Real-world social dynamics and power imbalances (especially between device owner employers and incidental user employees) may limit the effectiveness of these conversations, so these specific situations of incidental user experiences are important to explore further.

Make it easier for device owners to reduce the amount of data collected. Finally, considering that device owners' hesitation to accommodate others was often tied to their desire to maintain devices' beneficial uses, novel techniques could be developed to limit data collection without inhibiting these goals. For example, if a device owner could easily use a camera to monitor their own property without also capturing the public sidewalk or their neighbors' yards, this would potentially mitigate some privacy concerns. Figures 1, 4, and 5 also show proposed solutions from focus groups that limit data collection about incidental users. Notably, some of these solutions could be well-aligned with the concerns device owners had about incidental users interacting with their devices. For example, the participant-generated idea from Figure 5 was proposed not only to limit data collection about incidental users but also to prevent incidental users from triggering voice assistant commands that reveal private information about the device owner or result in unexpected financial charges.

Acknowledgements

We would like to thank our colleagues in CyLab for their feedback on the focus group and survey study designs and the writing in this paper. We thank Ronald and Dawn Cobb for their help making the logistical, behind-the-scenes aspects of one focus group session run smoothly. We also thank the reviewers and shepherd for their feedback and encouragement to improve this paper. This project was supported in part by a gift from CyLab.

References

[1] Prolific. https://www.prolific.co/.

[2] SmartThings. https://www.smartthings.com/.

[3] N. Abdi, K. M. Ramokapane, and J. M. Such. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)*, 2019.

[4] N. Apthorpe, Y. Shvartzshnaider, A. Mathur, D. Reisman, and N. Feamster. Discovering smart home internet of things privacy norms using contextual integrity. In *Proceedings of ACM Interaction Mobile Wearable Ubiquitous Technology (IMWUT)*, 2018.

[5] I. Bastys, M. Balliu, and A. Sabelfeld. If this then what? Controlling flows in IoT apps. In *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018.

[6] D. Bates, M. Mächler, B. Bolker, and S. Walker. Fitting linear mixed-effects models using lme4. *Journal of Statistical Software*, 67(1):1–48, 2015.

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

[8] S. S. Bhunia and M. Gurusamy. Dynamic attack detection and mitigation in IoT using SDN. In *Proceedings of the 27th IEEE International Telecommunication Networks and Applications Conference (ITNAC)*, 2017.

[9] N. Bowles. Thermostats, locks and lights: Digital tools of domestic abuse. *The New York Times*, June 2018.

[10] W. Brackenbury, A. Deora, J. Ritchey, J. Vallee, W. He, G. Wang, M. L. Littman, and B. Ur. How users interpret bugs in trigger-action programming. In *Proceedings of the 2019 Conference on Human Factors in Computing Systems (CHI)*, 2019.

[11] Z. B. Celik, P. McDaniel, and G. Tan. Soteria: Automated IoT safety and security analysis. In *Proceedings of the 2018 USENIX Annual Technical Conference*, 2018.

[12] Z. B. Celik, G. Tan, and P. McDaniel. IoTGuard: Dynamic enforcement of security and safety policy in commodity IoT. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS)*, 2019.

[13] C. Cobb, M. Surbatovich, A. Kawakami, M. Sharif, L. Bauer, A. Das, and L. Jia. How risky are real users' IFTTT applets? In *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS)*, 2020.

[14] N. J. Davis, H. Shishodia, B. Taqui, C. Dumfeh, and J. Wylie-Rosett. Resident physician attitudes and competence about obesity treatment: Need for improved education. *Medical Education Online*, 13(1):4475, 2008.

[15] N. DeMarinis and R. Fonseca. Toward usable network traffic policies for IoT devices in consumer networks. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy (IoTS&P)*, 2017.

[16] S. Demetriou, N. Zhang, Y. Lee, X. Wang, C. Gunter, X. Zhou, and M. Grace. Hanguard: SDN-driven protection of smart home WiFi devices from malicious mobile apps. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2017.

[17] P. Emami-Naeini, Y. Agarwal, L. Cranor, and H. Hibshi. Ask the experts: What should be on an IoT privacy and security label? In *Proceedings of the 41st IEEE Symposium on Security and Privacy (SP)*, 2020.

[18] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 Conference on Human Factors in Computing Systems (CHI)*, 2019.

[19] V. Fanelle, S. Karimi, A. Shah, B. Subramanian, and S. Das. Blind and human: Exploring more usable audio CAPTCHA designs. In *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS)*, 2020.

[20] E. Fernandes, J. Jung, and A. Prakash. Security analysis of emerging smart home applications. In *Proceedings of the 37th IEEE Symposium on Security and Privacy (SP)*, 2016.

[21] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash. Flowfence: Practical data protection for emerging IoT application frameworks. In *Proceedings of the 25th USENIX Security Symposium (USENIX Security)*, 2016.

[22] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash. Security implications of permission models in smart-home application frameworks. *IEEE Security Privacy Magazine*, 15(2):24–30, 2017.

[23] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash. Decentralized action integrity for trigger-action IoT platforms. In *Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS)*, 2018.

[24] A. Foster. When parents eavesdrop on nannies. https://www.nytimes.com/2019/08/19/opinion/nanny-cams-privacy.html, August 2019.

[25] G. A. Fowler. The doorbells have eyes: The privacy battle brewing over home security cameras. *The Washington Post*, 2019.

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

[27] G. M. Graff. Now a dorm room minecraft scam brought down the Internet. *Wired*, December 2017.

[28] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur. Rethinking access control and authentication for the home internet of things (IoT). In *Proceedings*

of the 27th USENIX Security Symposium, 2018.

[29] K.-H. Hsu, Y.-H. Chiang, and H.-C. Hsiao. Safechain: Securing trigger-action programming from attack chains. *IEEE Transactions on Information Forensics and Security*, 14(10):2607–2622, 2019.

[30] J. Huang and M. Cakmak. Supporting mental model accuracy in trigger-action programming. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, 2015.

[31] Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao, and A. Prakash. ContexIoT: Towards providing contextual integrity to appified IoT platforms. In *Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS)*, 2017.

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

[33] C.-J. M. Liang, L. Bu, Z. Li, J. Zhang, S. Han, B. F. Karlsson, D. Zhang, and F. Zhao. Systematically debugging IoT control system correctness for building automation. In *Proceedings of the 3rd ACM International Conference on Systems for Energy-Efficient Built Environments (BuildSys)*, 2016.

[34] C.-J. M. Liang, B. F. Karlsson, N. D. Lane, F. Zhao, J. Zhang, Z. Pan, Z. Li, and Y. Yu. Sift: Building an internet of safe things. In *Proceedings of the 14th International Conference on Information Processing in Sensor Networks (ISPN)*, 2015.

[35] S. Mare, L. Girvin, F. Roesner, and T. Kohno. Consumer smart homes: Where we are and where we need to go. In *HotMobile*, 2019.

[36] N. McDonald and A. Forte. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 Conference on Human Factors in Computing Systems (CHI)*, 2020.

[37] N. McDonald, S. Schoenebeck, and A. Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. In *Proceedings of the 22nd ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*, 2019.

[38] C. Nandi and M. D. Ernst. Automatic trigger generation for rule-based smart homes. In *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security (PLAS)*, 2016.

[39] D. T. Nguyen, C. Song, Z. Qian, S. V. Krishnamurthy, E. J. M. Colbert, and P. McDaniel. IotSan: Fortifying the Safety of IoT Systems. In *Proceedings of the 14th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT)*, 2018.

[40] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli. An experimental study of security and privacy risks with emerging household appliances. In *Proceedings of the 2014 IEEE Conference on Communications and Network Security*, 2014.

[41] S. S. Oh, J. A. Mayer, E. C. Lewis, D. J. Slymen, J. F. Sallis, J. P. Elder, L. Eckhardt, A. Achter, M. Weinstock, L. Eichenfield, L. C. Pichon, and G. R. Galindo. Validating outdoor workers' self-report of sun protection. *Preventive Medicine*, 39(4):798–803, 2004.

[42] D. Palmer. Mirai botnet adds three new attacks to target IoT devices. *ZDNet*, May 2018.

[43] R. Schuster, V. Shmatikov, and E. Tromer. Situational access control in the Internet of Things. In *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018.

[44] T. K. Shrirang Mare, Franziska Roesner. Smart devices in airbnbs: Considering privacy and security for both guests and hosts. *Proceedings on Privacy Enhancing Technologies*, Apr. 2019.

[45] A. K. Simpson, F. Roesner, and T. Kohno. Securing vulnerable home IoT devices with an in-hub security manager. In *Proceedings of the 15th IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017.

[46] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani. Network-level security and privacy control for smart-home IoT devices. In *Proceedings of the 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015.

[47] M. Surbatovich, J. Aljuraidan, L. Bauer, A. Das, and L. Jia. Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of IFTTT recipes. In *Proceedings of the 26th International World Wide Web Conference (WWW)*, 2017.

[48] M. Tabassum, T. Kosinski, and H. R. Lipford. "I don't own the data": End user perceptions of smart home device data practices and risks. In *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)*, 2019.

[49] Y. Tian, N. Zhang, Y.-H. Lin, X. Wang, B. Ur, X. Guo, and P. Tague. SmartAuth: User-centered authorization for the Internet of Things. In *Proceedings of the 26th USENIX Security Symposium*, 2017.

[50] Q. Wang, P. Datta, W. Yang, S. Liu, A. Bates, and C. A. Gunter. Charting the attack surface of trigger-action IoT platforms. In *Proceedings of the 26th ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019.

[51] Q. Wang, W. U. Hassan, A. Bates, and C. Gunter. Fear and logging in the internet of things. In *Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS)*, 2018.

[52] Y. Yao, J. R. Basdeo, O. R. Mcdonough, and Y. Wang. Privacy perceptions and designs of bystanders in smart homes. In *Proceedings of the 22nd ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*, 2019.

[53] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets)*, 2015.

[54] E. Zeng and F. Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *Proceedings of the 28th USENIX Security Symposium*, 2019.

[55] L. Zhang, W. He, J. Martinez, N. Brackenbury, S. Lu, and B. Ur. AutoTap: Synthesizing and repairing trigger-action programs using LTL properties. In *Proceedings of the 41st*

International Conference on Software Engineering (ICSE), 2019.

A Recruitment materials

This section includes the text that was posted to local online forums to recruit participants.

Research participants needed: Do your friends, family, or neighbors have smart home devices?

We are a group of researchers from [Institution Name] working to understand the effects of smart devices on users. We are looking for participants to take part in a group discussion. Are you at least 18 years old? Have you used a smart home device OR visited a home that had smart home device? (Devices include but are not limited to Amazon Echo, Google Home, Nest Thermostat, Ring Doorbell) In this voluntary study, you will be asked to: - Participate in a 90 minute group discussion at Carnegie Mellon University campus. - Talk about your experiences with and feelings about smart home devices. If you participate in the study, you will receive $30 in cash. Please fill out the survey in the [link]. If you are eligible, a researcher will reach out to schedule a time for you to participate.

B Survey instrument

This section shows the survey content (not formatting) as it would have been seen by most participants. Participants were additionally asked to enter their prolific ID and were given a primer on the four types of smart home devices we asked about, including examples and pictures of each. The survey concluded with demographic questions (omitted due to space constraints).

Which of these smart home devices have you seen at **your own home**?

- ☐ smart or Internet-connected cameras
- ☐ voice assistants
- ☐ smart lights, thermostats, plugs or door locks
- ☐ smart appliances and other types of smart home devices
- ☐ none of these devices

Which of these smart home devices have you seen at **a friend or family member's home**?

- ☐ smart or Internet-connected cameras
- ☐ voice assistants
- ☐ smart lights, thermostats, plugs or door locks
- ☐ smart appliances and other types of smart home devices
- ☐ none of these devices

Which of these smart home devices have you seen at **a neighbor's home**?

- ☐ smart or Internet-connected cameras
- ☐ voice assistants
- ☐ smart lights, thermostats, plugs or door locks
- ☐ smart appliances and other types of smart home devices
- ☐ none of these devices
- ☐ I don't live close enough to anyone to consider them a neighbor

Which of these smart home devices have you seen at **a short term rental (e.g. Airbnb)**?

- ☐ smart or Internet-connected cameras
- ☐ voice assistants
- ☐ smart lights, thermostats, plugs or door locks
- ☐ smart appliances and other types of smart home devices
- ☐ none of these devices
- ☐ I have not been to a short term rental (or it has been a long time since I have been to a short term rental)

Which of these smart home devices have you seen while you were at **someone else's home for work**?

- ☐ smart or Internet-connected cameras
- ☐ voice assistants
- ☐ smart lights, thermostats, plugs or door locks
- ☐ smart appliances and other types of smart home devices
- ☐ none of these devices
- ☐ I do not go into other people's homes for work

If you have seen smart home devices in other places or situations, please give a short description here: ☐

Devices in my own home Considering the smart home devices you have at **your own home**, which devices do you own? Please include devices that you feel ownership over, even if you share them with other people, but do not include devices purchased and installed by other people who might live with you.

- ☐ smart or Internet-connected cameras
- ☐ voice assistants
- ☐ smart lights, thermostats, plugs or door locks
- ☐ smart appliances and other types of smart home devices
- ☐ I do not own any of these devices

Considering the **privacy impacts** and **utility benefits** of each type of smart home device in **your own home**, how much do you (or do you think you would, if you have not seen this type of device at your own house) appreciate or dislike having this device around?

	Strongly dislike - It is not useful and/or makes me very concerned about my privacy	Dislike	Somewhat dislike	Neutral - I do not care whether it is there or not	Somewhat appreciate	Appreciate	Strongly appreciate - It is very useful and/or does not make me concerned about my privacy
smart or Internet-connected cameras	○	○	○	○	○	○	○
voice assistants	○	○	○	○	○	○	○
smart lights, thermostats, plugs or door locks	○	○	○	○	○	○	○
smart appliances and other types of smart home devices	○	○	○	○	○	○	○

[likert matrix, repeated later]

If you have taken any steps to make yourself feel more comfortable about smart home devices at your own home, please describe what you did: Reminder: please do not reveal any private or personally identifiable information about yourself or others ☐

Would you be willing to turn off your smart home devices or move them to a new location if you found out they were making

your neighbors uncomfortable? [Yes, No, It depends (please specify what factors would influence your choice)]

Would you be willing to turn off your smart home devices or move them to a new location if you found out they were making **someone else you live with** uncomfortable? [Yes, No, It depends (please specify what factors would influence your choice)]

Would you believe that not everyone pays attention in surveys? Please mark the answer choice 'it depends' and type **landlord** into the box. [Yes, No, It depends (please specify what factors would influence your choice)]

Would you be willing to turn off your smart home devices or move them to a new location if you found out they were making **a friend or family member who is visiting** your home uncomfortable? [Yes, No, It depends (please specify what factors would influence your choice)]

Would you be willing to turn off your smart home devices or move them to a new location if you found out they were making **someone working at your home** (e.g., package delivery person or babysitter) uncomfortable? [Yes, No, It depends (please specify what factors would influence your choice)]

Devices at my neighbors' homes

Considering the **privacy impacts** and **utility benefits** of each type of smart home device at **your neighbor's home**, how much do you (or do you think you would, if you have not seen this type of device at your neighbor's home) appreciate or dislike having this device around? [likert matrix, as before]

If you have taken any steps to make yourself feel more comfortable about smart home devices at your neighbors' homes, please describe what you did: Reminder: please do not reveal any private or personally identifiable information about yourself or others

Devices at my friends' homes

Considering the **privacy impacts** and **utility benefits** of each type of smart home device at **your friend or family member's home**, how much do you (or do you think you would, if you have not seen this type of device at your friend or family member's home) appreciate or dislike having this device around? [likert matrix, as before]

If you have taken any steps to make yourself feel more comfortable about smart home devices at friends' or family members' homes, please describe what you did: Reminder: please do not reveal any private or personally identifiable information about yourself or others

Devices I've seen while working Considering the **privacy impacts** and **utility benefits** of each type of smart home device at **a home where you were working**, how much do you (or do you think you would, if you have not seen this type of device at a home where you were working) appreciate or dislike having this device around? [likert matrix, as before]

If you have taken any steps to make yourself feel more comfortable about smart home devices at homes where you were working, please describe what you did: Reminder: please do not reveal any private or personally identifiable information about yourself or others

Devices I've seen at an Airbnb Considering the **privacy impacts** and **utility benefits** of each type of smart home device at **a short term rental (e.g., Airbnb)**, how much do you (or do you think you would, if you have not seen this type of device at a short term rental) appreciate or dislike having this device around? [likert matrix, as before]

If you have taken any steps to make yourself feel more comfortable about smart home devices at short term rentals, please describe what you did: Reminder: please do not reveal any private or personally identifiable information about yourself or others

Evaluating solution characteristics

Imagine a situation in which **a smart home device that *someone else* owns causes you to feel uncomfortable about your privacy** (i.e., because the device could collect data about you). If someone came up with a solution to help you feel more comfortable about this smart home device, what characteristics should the solution have? **Please rank the following characteristics from most to least important** by dragging each of the items from the left into one of the three boxes on the right. Put the characteristics you care most about at the top.

The solution should ... • Let me know what data nearby devices will actually collect • Let me know when a device is present • Let me know when nearby devices are currently collecting data • Let me know what type of data nearby devices are capable of collecting • Give me a chance to avoid data collection • Give me a chance to adapt my behavior • Conform to social conventions (e.g., not require anyone to do something that would be seen as rude) • Let me know exactly where a device is located • Require minimal effort from me • Place this block in "These characteristics are somewhat important to me" to let us know that you are paying attention. • Require minimal effort from the device owner

[Boxes on the right: These characteristics are very important to me | These characteristics are somewhat important to me | I don't care if the solution has this characteristic]

If there are other characteristics that you think a solution should or should not have, please describe them here: []

Reminder: please do not reveal any private or personally identifiable information about yourself or others

Demographics

Please complete the following demographic questions to finish this survey. What is your age? [under 18, 18-29, 30-49, above 50, I prefer not to answer.]

Who lives in your house? (Please check all that apply) [No one (I live alone), Roommates, Spouse, Parents, Children, Extended Family, Pets, Other, I prefer not to answer]

What is your gender? [Male, Female, Non-binary, Write-in, I prefer not to answer]

Which of the following best describes you? [Asian or Pacific Islander, Black or African American, Hispanic or Latino, Native American or Alaskan Native, White or Caucasian, Multiracial or Biracial, A race/ethnicity not listed here, I prefer not to answer]

What is your highest level of education? [Less than a high school diploma, High school degree or equivalent (e.g. GED), Some college, no degree, Associate degree (e.g. AA, AS), Bachelor's degree (e.g. BA, BS), Master's degree (e.g. MA, MS, MEd),

Professional degree (e.g. MD, DDS, DVM), Doctorate (e.g. PhD, EdD), I prefer not to answer]

What is your current employment status? (Please check all that apply) [Employed full time (40 or more hours per week), Employed part time (up to 39 hours per week), Unemployed, Student, Retired, Homemaker, Self-employed, I prefer not to answer]

What is your profession? [ ]

Reminder: please do not reveal any private or personally-identifiable information about yourself or others in your written answers

What is your household annual income? [0-$49,999, $50,000-$99,999, $100,000-$149,999, $150,000-$199,999, $200,000 and above, I prefer not to answer]

Have you ever purchased, installed, or configured a smart home device before? [Yes, No]

If you have any questions or comments about the study, please leave them here.

Reminder: please do not reveal any private or personally-identifiable information about yourself or others in your written answers

C Statistical analyses

Table 6 describes the results of the generalized linear mixed model regression we built to study factors correlated with participants' general appreciation of the presence of smart home devices. In this table, a positive coefficient indicates higher likelihood of appreciating a smart home devices and a negative coefficient indicates a higher likelihood of having privacy concerns.

Tables 7, 8, 9, and 10 show the results of the logistic regression models modeling the factors correlated with the willingness to accommodate neighbors, housemates, friends, and workers in people's homes. In these tables, a positive coefficient indicates a higher likelihood of being willing to accommodate others, and a negative coefficient indicates a lower likelihood.

All of the tables in this appendix use the abbreviation *DO* for *device owner* and *IU* for *incidental user*, and they use a * to denote statistically significant results.

	baseline	*coef.*	*std.err.*	*t*	*p*
(Intercept)		**4.800**	**0.655**	**7.325**	**<0.001**
Situation: friend's home	own home	0.144	0.137	1.053	0.292
Situation: neighbor's home	**own home**	**1.040**	**0.144**	**7.205**	**<0.001***
Situation: rental	**own home**	**-1.190**	**0.128**	**-9.310**	**<0.001***
Situation: work	**own home**	**0.366**	**0.135**	**2.703**	**0.007***
Device: camera	**appliances**	**-3.116**	**0.140**	**-22.265**	**<0.001***
Device: lights	appliances	0.079	0.150	0.528	0.597
Device: voice	**appliances**	**-2.183**	**0.137**	**-15.897**	**<0.001***
Real experience?: yes	**no**	**0.940**	**0.117**	**8.052**	**<0.001***
DO or IU?: DO only	both	0.089	0.735	0.122	0.903
DO or IU?: IU only	**both**	**-2.164**	**0.347**	**-6.421**	**<0.001***
DO or IU?: neither	**both**	**-2.043**	**0.632**	**-3.230**	**0.001***
Gender: male	female	-0.344	0.280	-1.228	0.219
Gender: non-binary	**female**	**-2.894**	**1.340**	**-2.159**	**0.031***
Gender: genderfluid	female	-0.989	2.466	-0.401	0.688
Gender: no answer	female	-5.726	3.509	-1.632	0.103
Age: 30-49	18-29	-0.322	0.387	-0.831	0.411
Age: 50+	18-29	0.019	0.387	0.050	0.960
Age: no answer	18-29	1.100	2.353	0.467	0.640
Race: Black	Asian	1.131	0.621	1.820	0.069
Race: Hispanic	Asian	0.298	0.714	0.416	0.677
Race: Multi	Asian	-0.519	1.078	-0.482	0.630
Race: Native	Asian	-0.018	1.944	-0.009	0.993
Race: White	Asian	-0.322	0.505	-0.638	0.523
Race: Other	Asian	2.637	2.234	1.180	0.278
Race: no answer	Asian	-0.542	2.751	-0.197	0.844
Income: $0-$49,999	$100,000-$149,999	-0.221	0.449	-0.493	0.622
Income: $50,000-$99,999	$100,000-$149,999	0.234	0.430	0.543	0.587
Income: $150,000-$199,999	$100,000-$149,999	-0.009	0.691	-0.013	0.990
Income: $200,000+	$100,000-$149,999	0.170	0.761	0.223	0.823
Income: no answer	$100,000-$149,999	-0.986	1.210	-0.815	0.415

Table 6. Generalized linear mixed model (GLMM) regression output describing how features of a scenario and people's demographics are related to their appreciation of the presence of a smart home device.

	baseline	*coef.*	*std.err.*	*t*	*p*
(Intercept)		**0.790**	**0.136**	**5.793**	**<0.001***
Overall positive appreciation		**-0.021**	**0.006**	**-3.586**	**<0.001***
DO or IU?: DO only	both	0.053	0.137	0.390	0.697
DO or IU?: IU only	both	0.020	0.068	0.287	0.774
DO or IU?: neither	both	0.051	0.123	0.418	0.676
Gender: male	female	0.046	0.051	0.892	0.373
Gender: non-binary	female	-0.274	0.253	-1.080	0.281
Gender: genderfluid	female	0.467	0.496	0.941	0.347
Gender: no answer	female	0.378	0.397	0.951	0.342
Age: 30-49	18-29	-0.003	0.070	-0.044	0.965
Age: 50+	18-29	0.049	0.069	0.710	0.478
Age: no answer	18-29	-0.179	0.394	-0.454	0.650
Income: $0-$49,999	$100,000-$149,999	-0.068	0.083	-0.823	0.411
Income: $50,000-$99,999	$100,000-$149,999	-0.099	0.079	-1.249	0.212
Income: $150,000-$199,999	$100,000-$149,999	0.080	0.129	0.623	0.534
Income: $200,000+	$100,000-$149,999	0.055	0.141	0.390	0.697
Income: no answer	$100,000-$149,999	-0.020	0.207	-0.097	0.923

Table 7. Logistic regression model describing how participants' overall appreciation of smart home devices and their demographics are related to their likelihood of being willing to turn off devices **for their neighbors**.

	baseline	*coef.*	*std.err.*	*t*	*p*
(Intercept)		**1.142**	**0.097**	**11.751**	**<0.001***
Overall positive appreciation		**-0.016**	**0.004**	**-3.919**	**<0.001***
DO or IU?: DO only	both	-0.032	0.098	-0.328	0.743
DO or IU?: IU only	both	-0.005	0.049	-0.095	0.924
DO or IU?: neither	both	-0.028	0.088	-0.314	0.754
Gender: male	female	0.023	0.037	0.633	0.527
Gender: non-binary	female	-0.002	0.181	-0.011	0.991
Gender: genderfluid	female	0.049	0.355	0.137	0.891
Gender: no answer	female	0.371	0.284	1.306	0.193
Age: 30-49	18-29	-0.086	0.050	-1.715	0.087
Age: 50+	18-29	-0.091	0.049	-1.853	0.065
Age: no answer	18-29	-0.502	0.281	-1.784	0.075
Income: $0-$49,999	$100,000-$149,999	-0.023	0.059	-0.396	0.692
Income: $50,000-$99,999	$100,000-$149,999	0.068	0.056	1.209	0.227
Income: $150,000-$199,999	$100,000-$149,999	0.117	0.092	1.277	0.202
Income: $200,000+	$100,000-$149,999	0.113	0.101	1.124	0.262
Income: no answer	$100,000-$149,999	-0.145	0.148	-0.981	0.327

Table 8. Logistic regression model describing how participants' overall appreciation of smart home devices and their demographics are related to their likelihood of being willing to turn off devices **for their housemates**.

	baseline	*coef.*	*std.err.*	*t*	*p*
(Intercept)		**1.034**	**0.120**	**9.469**	**<0.001***
Overall positive appreciation		**-0.023**	**0.005**	**-4.471**	**<0.001***
DO or IU?: DO only	both	-0.044	0.120	-0.369	0.712
DO or IU?: IU only	both	-0.076	0.060	-1.274	0.203
DO or IU?: neither	both	-0.168	0.108	-1.561	0.119
Gender: male	female	-0.064	0.045	-1.421	0.156
Gender: non-binary	female	0.055	0.223	0.248	0.804
Gender: genderfluid	female	0.074	0.436	0.170	0.865
Gender: no answer	female	0.224	0.349	0.641	0.522
Age: 30-49	18-29	-0.061	0.062	-0.981	0.327
Age: 50+	18-29	-0.085	0.061	-1.394	0.164
Age: no answer	18-29	-0.480	0.346	-1.384	0.167
Income: $0-$49,999	$100,000-$149,999	0.097	0.073	1.332	0.184
Income: $50,000-$99,999	$100,000-$149,999	0.097	0.070	1.388	0.166
Income: $150,000-$199,999	$100,000-$149,999	0.074	0.115	0.638	0.524
Income: $200,000+	$100,000-$149,999	0.094	0.124	0.757	0.450
Income: no answer	$100,000-$149,999	0.154	0.182	0.845	0.399

Table 9. Logistic regression model describing how participants' overall appreciation of smart home devices and their demographics are related to their likelihood of being willing to turn off devices **for their friends**.

	baseline	*coef.*	*std.err.*	*t*	*p*
(Intercept)		**1.080**	**0.133**	**8.143**	**<0.001***
Overall positive appreciation		**-0.025**	**0.006**	**-4.424**	**<0.001***
DO or IU?: DO only	both	-0.200	0.133	-1.502	0.134
DO or IU?: IU only	both	-0.044	0.067	-0.652	0.515
DO or IU?: neither	both	0.095	0.119	0.794	0.427
Gender: male	female	0.034	0.050	0.485	0.501
Gender: non-binary	female	0.292	0.246	1.188	0.236
Gender: genderfluid	female	0.259	0.483	0.538	0.591
Gender: no answer	female	0.316	0.386	0.818	0.414
Age: 30-49	**18-29**	**-0.204**	**0.069**	**-2.965**	**0.003***
Age: 50+	**18-29**	**-0.264**	**0.067**	**-3.915**	**<0.001***
Age: no answer	18-29	-0.474	0.383	-1.238	0.217
Income: $0-$49,999	$100,000-$149,999	-0.046	0.080	-0.570	0.569
Income: $50,000-$99,999	$100,000-$149,999	-0.027	0.077	-0.350	0.726
Income: $150,000-$199,999	$100,000-$149,999	-0.068	0.125	-0.542	0.588
Income: $200,000+	$100,000-$149,999	0.066	0.137	0.482	0.630
Income: no answer	$100,000-$149,999	0.075	0.201	0.374	0.709

Table 10. Logistic regression model describing how participants' overall appreciation of smart home devices and their demographics are related to their likelihood of being willing to turn off devices **for workers in their homes**.