Who Cares? Contextual Privacy Judgments from Owner and Bystander Perspectives in Different Smart Home Situations

Alisa Frik
International Computer Science Institute
afrik@icsi.berkeley.edu

Xiao Zhan
King's College London
xiao.zhan@kcl.ac.uk

Noura Abdi
Liverpool Hope University
abdin@hope.ac.uk

Julia Bernd
International Computer Science Institute
jbernd@icsi.berkeley.edu

Abstract

Current privacy protections for smart home devices rarely consider bystanders' privacy, whose preferences are varied and may differ from primary users. We use Contextual Integrity theory to explore context-dependent variation in privacy norms regarding smart home bystanders' data. We conducted a vignette-based survey with 761 participants in the US, varying parameter values to capture acceptability judgments regarding bystander information flows in certain situations: domestic work, shared housing, visiting a friend overnight, and Airbnb. We found that recipients and purposes of sharing impact acceptance the most. Sharing interaction logs was more acceptable than audio or video. Sharing smart speaker data was less acceptable than smart camera or smart door lock data. We found nuanced interaction effects between factors in different smart home situations, and differences between protections most favored by participants playing bystander vs. owner roles. We provide design and policy recommendations for smart home privacy protections that consider bystanders' needs.

Keywords

Privacy Norms, Contextual Integrity, Bystanders, Smart Homes, Internet of Things, Ubiquitous Technology

1 Introduction

Only 15% of US consumers in a large 2023 survey did not own smart home devices [109]. This high adoption rate suggests that any privacy risks arising from smart home devices have a wide impact on society. Prior work has studied people's privacy concerns about smart home devices that they own [e.g. 1, 33, 40, 76, 88, 90], and about devices they do not own, but that they interact with or come in contact with, and that collect data about them [e.g. 26, 80, 86, 130] (hereafter we refer to people in this position as *bystanders*). Studies have shown diverging privacy expectations and preferences between device owners and bystanders [e.g. 3, 16, 36, 117]. However, current privacy mechanisms and regulations (such as GDPR [47] and CCPA [95]) primarily focus on protecting privacy of primary users, and have limited or no explicit provisions for bystander privacy. Our study therefore compares the two perspectives, to identify potential disconnects and points of alignment between views of device owners vs. bystanders that impact how privacy protections should be implemented in smart home systems, and assesses contextual variation in those views.

Prior work on bystanders' privacy has considered their privacy concerns, expectations, and preferences, but there is a lack of understanding about the *social norms* around collection of bystanders' data by smart home technologies. At the same time, prior empirical work has repeatedly demonstrated how privacy attitudes of primary users of smart home or Internet of Things (IoT) devices are dependent on context [23, 58, 71, 90]. However, there is a lack of understanding of contextual variations in opinions about bystanders' data. Contextual Integrity (CI) theory [75, 92, 94] has become the most commonly recognized theoretical foundation for researching the context-dependency of privacy. Thus, we rely on CI theory as the basis for the main part of our study, exploring contextual variations in acceptability judgments about bystanders' data, which can provide a basis for exploring privacy norms. (See §3.4 for discussion of the uses and limitations of empirical measurement for inferring norms.) CI defines *privacy norms* as social norms about appropriate flows of information in a particular context.

Our research questions are as follows:

- **RQ1:** When are flows of information collected about bystanders by smart home devices viewed as acceptable?
- **RQ2:** How does acceptability of data flows about bystanders vary (if at all) across contexts and scenarios?
- **RQ3:** Do participants' individual characteristics and experiences (socio-demographics, prior experiences with smart home devices, etc.) affect their acceptability judgments?
- **RQ4:** What privacy controls for bystander data do participants want to have?
- **RQ5:** How do these desired privacy controls differ (if at all) across contexts and scenarios?

To answer RQ1–RQ3, about contextual privacy judgments, we ran a vignette-based survey with 761 participants residing in the US. To answer RQ4–RQ5, we explicitly asked participants about privacy control mechanisms.

In the vignettes, each participant was presented with a scenario in which they played the role of either a device owner or a bystander in one of four types of situations, involving different relationships between owner and bystander: domestic work, shared housing, or overnight stays at either a friend's house or a short-term rental property booked on Airbnb. The scenarios also varied by device type and the owner's disclosure behavior. We then presented participants

Proceedings on Privacy Enhancing Technologies 2025(3), 106–134

https://doi.org/10.56553/popets-2025-0091

with a series of vignettes with varied data formats, recipients, and purposes of sharing.

We found that recipients, purposes of sharing, and their interaction effects played the most important role in acceptance of flows of bystanders' data. Logs of bystanders' interactions with devices were more appropriate to share than audio or video. Smart locks and smart speakers were associated with higher and lower acceptance than smart cameras, respectively, in some regression models. Differences between the privacy judgments of participants assigned the bystander vs. the device owner role were not statistically significant, nor were differences between situations and transparency levels. However, we found some significant interaction effects between situations and other contextual parameters, and small differences in the distribution of qualitative responses about desired privacy controls between participants in the role of bystanders vs. owners, as well as between different device types and situations.

Based on our findings, we make recommendations for smart home developers about enabling more agency for bystanders—even where there are power differentials or social barriers.

Our study makes the following main contributions:

- While prior work has studied concerns and preferences of bystanders in smart homes [e.g. 10, 36, 79, 125], we use acceptability judgments to explore *privacy norms* regarding the acceptance of various flows of bystanders' data.
- While prior work has studied acceptability of flows of data collected by IoT devices about primary users [e.g., 2, 19, 20, 58, 89], we make a novel contribution by empirically exploring contextual variations in acceptability with a focus on *bystanders' data* collected by smart home devices.
- We compare people's views as bystanders and device owners on data flows and desired privacy controls for smart home bystanders, to identify potential disconnects and alignments.
- We provide recommendations regarding privacy protections for bystanders to smart home data collection, based on participants' desired controls, accounting for perspectives as both device owners and bystanders.

2 Related Work

Prior work has studied privacy experiences, concerns, and preferences of primary users in smart homes [e.g. 1, 23, 63, 70, 76, 132], including users' coping strategies [1, 7, 45, 132], and has provided design recommendations for smart home privacy controls for primary users. Research has also explored privacy concerns of *bystanders* in smart homes, and contextual factors affecting those concerns [e.g. 16, 78, 80, 81, 86, 134, 135] [overview in 100]. Despite this research, the factors driving device owners' and bystanders' expectations and norms about data practices are not fully understood. Our study takes a contextual approach to understanding such perspectives.

2.1 Privacy in Multi-User Smart Homes

On the one hand, smart home devices in multi-user environments can provide opportunities for shared experiences and connection [18]. On the other hand, they raise privacy concerns among secondary users and other bystanders, and limit their control over personal information. Generally, smart home bystander privacy can be seen as an example of interdependent privacy [28] [overviews in 62, 111], in that bystanders' privacy depends on device owners' decisions about device deployment and configuration of settings that may result in the access, use, and sharing of bystanders' data, often occurring without their knowledge or consent. In the case of multi-user smart homes, secondary users may influence such decisions, but still be essentially dependent on primary users' discretion.

One important factor in multi-user smart homes is having appropriate consent mechanisms for bystanders [32, 129]; however, existing controls fail to request such consent, raising privacy concerns among bystanders [31]. Avoidance and acceptance are two main strategies for users of shared smart speakers to cope with privacy risks [61, 86]. Zeng et al. [131] identified gaps between the functionalities of smart home devices and the security and privacy concerns of those that use them, and suggested that device manufacturers and researchers focus on multi-user scenarios to better understand which controls different users may need.

Some prior studies have explicitly compared the perspectives of owners and bystanders, or participants playing those roles, on various aspects of smart home privacy. For example, Alshehri et al. [15, 16] explored the perspectives of device owners and bystanders on privacy concerns, expectations of disclosures by device owners, willingness to share bystanders' data with owners, and negotiation behaviors. Similarly, while Zhou et al. [135]'s study involved scenarios from both owner and bystander perspectives, and explored contextual variables and relationships, their goal was to model and support negotiations about having devices on/off, not norms for data sharing. Thakkar et al. [117] and Marky et al. [79] specifically compared views of participants taking owner vs. bystander roles on some proposed bystander privacy mechanisms. Several other studies described in §2.2 also looked at multiple perspectives, but again, they were not concerned with isolating and quantifying factors that affect the acceptability of information sharing.

Prior research has highlighted the influence of socioeconomic and demographic factors on views of smart home devices [22, 67, 110, 126]. For example, a study about smart home privacy found participants across four countries were largely more concerned about devices in their own homes vs. other people's homes, but that specific concerns varied between the two contexts [41]. It also found that non-male participants were less likely to have configured smart devices, including privacy settings, whether or not they were the most frequent user. Thus, we included socioeconomic and demographic factors in our study as control variables.

2.2 Considerations in Specific Bystander Situations/Relationships

Prior work studied a variety of relationships and power dynamics in smart homes [e.g. 26, 52, 72, 106, 115, 129]. Often relationships and trust between users in a multi-smart home have a significant effect on who has access to the device [68]. The most commonly studied multi-user smart home situations involve family dynamics [e.g. 27, 51, 61, 118], often reflected in differences between primary and secondary users, especially among couples [43, 66]. Below we review several other relationships and situations that have been researched, inspiring our study.

2.2.1 Housemates. Prior work exploring the dynamics between housemates in a smart home [52] found that tensions regarding the control of the smart home device often arise between housemates. In such conflicts, the owner or installer of the device usually has more agency, and the final word regarding use and configuration of the device. Often these conflicts are due to a lack of existing controls, as smart home technologies are not designed with multi-user contexts in mind, in particular multiple people sharing the same space [70, 132]. Privacy concerns also play a key role in a shared housing setting, often due to lack of understanding about data flows between device owners and housemates [61].

2.2.2 *Visitors and Guests.*

Several studies have examined guests visiting smart homes (though generally not overnight stays, as in our study). In interviews with visitors, cohabitants, and owners of smart speakers, Meng et al. [86] found that they have similar attitudes, and social norms (or "smart speaker etiquette") help manage boundaries, primarily based on trust. Cobb et al. [36] found that tensions between primary and incidental smart home users are often due to privacy concerns around surveillance and data collection, compounded by the lack of privacy controls designed for multi-users and bystanders. Other studies examined visitors' comfort, privacy perceptions, and coping mechanisms [80, 83, 117]. Trust and the closeness of the relationship between homeowner and guest is found to impact guests' comfort with the device [83, 130, 135]—but also their desire for privacy protections [15, 16, 32]. Although some work has been done to explore appropriate privacy controls for guests in smart homes [e.g. 39, 79, 82, 117, 130], with some uptake in industry (see §5.3), the desire for guest privacy controls is still largely unsatisfied in practice.

2.2.3 *Short-Term Rentals.*

The privacy of guests in short-term rentals such as Airbnbs also raised concerns, because smart devices in Airbnbs have been used in a harmful manner, e.g., for surveillance of guests [54, 108]. Mare et al. [78] found that both Airbnb guests and hosts had diverse privacy views, often leading to mismatched expectations. They also found discrepancies in mental models of device data flows. Dey et al. [42] found that a perceived competitive advantage in giving guests remote access to the home—which also helps protect the properties from misuse—outweighed concerns about guests' privacy for interviewed Airbnb hosts. Wang et al. [125] explored Airbnb guests' preferences regarding reasons, timing, processes, and channels for privacy negotiations.

2.2.4 *Domestic Workers.*

Domestic workers employed in smart homes have diverse privacy concerns, but are often unwilling to discuss them with the employers due to power differentials or worries it might raise concerns about the integrity of their work [3]. The power imbalances and social norms make it difficult for domestic workers to challenge employers' decisions [26, 64, 65]. While nannies understand employers' desire to have cameras, they express a desire to be at least informed about their presence [3, 26]. Similarly, caregivers often view security cameras as undermining the trust required for them to successfully give care, while exacerbating power inequalities [64]. Albayaydh and Flechais [10, 12] proposed a privacy protection app to address privacy concerns of domestic workers and power dynamics in smart homes. They showed that religious and social norms play a role in tensions between domestic workers and smart home owners in Jordan [10, 11, 13].

2.2.5 *Comparing Situations.*

Some of the research described above drew explicit comparisons between different types of bystander situation or relationship with device owners. For example, Cobb et al. [36] found that incidental users were less comfortable with smart home devices in short-term rentals than in their own homes or homes where they worked. Thakkar et al. [117] note that participants were more comfortable with devices in homes they were visiting than devices of family members in their own household, if the bystander in the latter case was working from home—demonstrating the need to consider detailed nuances when interpreting privacy attitudes. Yao et al. [130] note that participants in their qualitative study had varied views depending on the bystander scenario they were responding to (Airbnb, playdate as a guest, own home), particularly in terms of how much exposure was implied. Their findings suggest a need for further exploration, and quantification, of these variations. Chiang et al. [32] compared several owner-bystander relationships, finding that participants had the strictest consent requirements for data collection by devices owned by co-habitants, compared to short-term rental hosts or clients of a maintenance worker. They also found differences in consent requirements by device type and data format, but did not conduct factorial analysis.

A Need for Nuance. Overall, while primary users of smart home devices may wish to give domestic workers, guests, and family different privacy controls to suit those relationships, such options are not always available [e.g. 132]. This lack may lead to conflicts, for example, regarding perceived surveillance and decisions about devices [e.g. 16, 52, 87]. Thus it is important to continue exploring bystanders' attitudes and social norms about privacy in specific types of smart home environments, to design appropriate controls and mitigation strategies.

2.3 Context in Smart Home Privacy Perceptions

Several studies have focused on the context dependency of smart home or IoT users' privacy perceptions [23, 58, 71, 90]. For example, He et al. [58] found that primary users' perceptions of data sharing in multi-user smart homes depend on recipients and data types more than device types. Similarly, Abdi et al. [2] found that primary users' acceptance depended on data type, recipient type, purpose, and transmission principles. While these studies provide an interesting point of comparison, our study explores additional dimensions.

The Theory of Privacy as Contextual Integrity (CI) provides a framework for studying privacy preferences, expectations, and norms [25, 75, 92–94]. It views privacy perceptions in terms of appropriateness of information flows based on social norms in a specific situation. CI describes information flows using five parameters: sender, information type, data subject, recipient, and transmission principles. Prior quantitative work has used CI to explore privacy norms [e.g. 20, 84, 105, 133], including in smart homes [e.g. 2, 19, 89], and to model smart home privacy threats [e.g. 29].

Differences from Prior Work. Most closely related are the studies of Apthorpe et al. [19], He et al. [58], Abdi et al. [2], and Musale and Lee [89], which all used factorial vignettes to explore appropriateness of flows of information collected by smart home devices.

We use a similar factorial vignette methodology in our survey, but we have several important differences in study design. First, we focus on the information collected by smart home devices *about bystanders*, which most prior work has not. The exception is Musale and Lee [89], who compared acceptability of data flows about the owner vs. other occupants of the house. Their participants, who were asked to play the role of device owners, had similar opinions regardless of data subject; however, they did not examine views on data about non-occupants (which we do).

Second, in addition to bystanders as a data subject, we examine a *different set of contextual parameters*, including a subset of devices and transmission principles used in Apthorpe et al. [19], but with a diverging set of recipients, data formats, and purposes not examined in the prior studies [2, 19, 58, 89].

Third, we explore the differences in acceptability judgments about flows of bystander data *between the perspectives* of bystanders and device owners, while those studies did not consider different perspectives, focusing only on opinions of primary users.

Finally, in contrast to prior work, our study explores the impact of *different situations or relationships* between primary users and bystanders (e.g. in an Airbnb scenario vs. an overnight stay at a friend's house) on privacy views.

The literature reviewed above highlights the importance of examining the impact of contextual factors on privacy norms in smart homes. Our work applies CI theory to better understand the privacy norms around bystanders' data, and expands quantified empirical evidence about such norms, supporting nuanced recommendations for smart home device developers and policymakers.

3 Methods

We ran a factorial vignette–based survey to examine how contextual factors affect acceptability judgments about sharing smart home bystanders' data. Vignettes are concise descriptions of situations with systematically varied parameters, used to compare respondents' views about aspects of the presented scenarios [2, 19, 50].

3.1 Vignettes and Survey Design

Table 1 lists the seven parameters that we varied in our study. To avoid participant fatigue and confusion, we used a hybrid between/within subjects approach, in which we asked participants to imagine themselves in a particular overall *scenario*, and then consider how their answers would change depending on specific data practices that varied between *vignettes*.

Each participant was presented with only one randomly assigned scenario, including four parameters that varied *between* subjects. They were assigned one of three *Devices*, and they played the *Role* of either a device owner or a bystander, in one of the four *Situations*. Participants saw a description of the device (see Appendix B) before the scenarios. The scenario also mentioned the owner's level of *Transparency* about the existence and data practices of the device.

We then presented each participant with several vignettes in random order, in which we varied three parameters *within* subjects: the *Data formats* the device collected, the *Recipients* with whom the data was shared, and for what *Purposes* it was shared. For each vignette, we asked participants to respond on a 5-point Likert scale how acceptable would it be if the specific data about a bystander captured by the device was shared with a particular recipient for different purposes (presented in random order). Scenarios and vignettes were constructed from frame sentences with parameter values from Table 1, as follows.

For participants that were assigned a **bystander** Role:

> *[Scenario:]* Imagine that you are a(n) [BYSTANDER'S ROLE]. Your [OWNER'S ROLE] installed a [DEVICE] in a common space inside the smart home that collects information about people in the home, including you. Your [OWNER'S ROLE] [TRANSPARENCY]. Next we will show you different scenarios that could happen in this situation, and ask how acceptable those scenarios are. Please read carefully, as this text won't change but scenarios below will vary slightly.
>
> *[Vignette:]* How acceptable would it be if [DATA FORMAT] of you captured by the [DEVICE] was shared with [RECIPIENT], for the following purposes? [LIST OF PURPOSES]

Example: Imagine that you are ***a housemate*** *in* ***a shared rental smart home****. Your* ***housemate Jackie*** *installed* ***a smart home camera*** *in a common space that collects information about people in the home, including* ***you****.* ***Your housemate Jackie told you the smart home camera is present but didn't explain details of data collection, use, sharing, and storage****.*

How acceptable would it be if ***a video of you*** *captured by* ***the smart home camera*** *was shared with* ***a third-party company's employees****, for the following purposes?*

For participants that were assigned a **device owner** Role:

> *[Scenario:]* Imagine that you are a(n) [OWNER'S ROLE]. You installed a [DEVICE] in a common space inside the smart home that collects information about people in the home, including your [BYSTANDER'S ROLE]. You [TRANSPARENCY] your [BYSTANDER'S ROLE]. Next we will show you different scenarios that could happen in this situation, and ask how acceptable those scenarios are. Please read carefully, as this text won't change but scenarios below will vary slightly.
>
> *[Vignette:]* How acceptable would it be if [DATA FORMAT] of your [BYSTANDER'S ROLE] captured by the [DEVICE] was shared with [RECIPIENT], for the following purposes? [LIST OF PURPOSES]

Example: Imagine that you are ***a host*** *of a* ***smart home you rented out on Airbnb****. You installed* ***a smart door lock*** *in a common space inside the smart home that collects information about people in the home, including* ***your Airbnb guest****. You told* ***your Airbnb guest the smart door lock is present and explained details of data collection, use, and sharing****.*

How acceptable would it be if ***logs/history of interactions with (records of when and how your Airbnb guest used) the smart door lock*** *was shared with* ***a government entity****, for the following purposes?*

Selection of Parameters*.* The parameters and values in our vignettes and scenarios were selected based on some of the information flow parameters identified in CI theory [92, 94], as well as on contextual factors identified in other prior work that touches on

Table 1: Scenario and vignette parameters. Parameters marked with * were fixed per participant.

Parameters	Values
Role* and Situation*	*For participants that were assigned a bystander Role:* - *Shared housing:* a housemate in a shared rental smart home *(bystander)* / housemate Jackie *(device owner)* - *Airbnb rental:* a guest in a smart home you rented on Airbnb *(bystander)* / Airbnb host *(device owner)* - *Overnight stay:* an overnight guest in a friend's smart home *(bystander)* / host *(device owner)* - *Domestic work:* a domestic worker in your employer's smart home *(bystander)* / employer *(device owner)* *For participants that were assigned a device owner Role:* - *Shared housing:* a housemate in a shared rental smart home *(device owner)* / housemate Adrian *(bystander)* - *Airbnb rental:* a host of a smart home you rented out on Airbnb *(device owner)* / Airbnb guest *(bystander)* - *Overnight stay:* a host of a friend visiting your smart home overnight *(device owner)* / guest *(bystander)* - *Domestic work:* an employer of a domestic worker in your smart home *(device owner)* / domestic worker *(bystander)*
Device*	- smart home camera - smart speaker - smart door lock
Transparency*	- did not tell - told and explained details of data collection, use, sharing, and storage - told but didn't explain details of data collection, use, sharing, and storage
Data format	- video - audio - logs/history of interactions with (records of when and how [bystander's Role] used) the device
Recipient	- the [device owner's Role] - a government entity - the employees of the company that made the device - a third-party company's employees - the device owner's contacts (e.g. friends, family, neighbors, etc.).
Purpose of Sharing	- to ensure the safety of the people in the home - to troubleshoot or improve the performance of the device - to assist in investigating a crime - to enforce house rules (e.g., about pets or noise) - to provide customized service/product recommendations - to share a memory - to monitor work

acceptability of information flows, including quantitative studies on norms or preferences for primary users' data [e.g. 2, 19, 20, 77, 90] and prior, mostly qualitative, work on bystander or multi-user situations [e.g. 3, 10, 26, 36, 41, 52, 61, 78, 131, 132].

Specifically, Data formats and Recipients reflect the *information type* (or *attribute*) and *recipient* parameters from the CI approach, respectively, while Purpose of sharing and Transparency parameters can be categorized as *transmission principles.* CI's *data subject* parameter is instantiated as the bystander in our study, and is fixed across all vignettes. We did not explicitly mention the final CI parameter, the *data sender*, in the vignettes, because the likely sender was largely implied by the Recipient. For example, when sharing with a government entity, the most likely sender would be the company that made the device, while when sharing with the owner's contacts, the sender is likely to be the device owner. However, in the exit survey, we asked participants about general acceptance of different data senders.

The location of the device and its data retention policies can also be considered *transmission principles* in CI theory. However, they have been widely explored in prior research, reaching a relative consensus that people prefer shorter data retention periods, are more concerned about data collection in private spaces (inside the house) than public spaces (e.g. on a porch), and are especially concerned about rooms for private activities (e.g., bathrooms and bedrooms), while views on devices in common spaces within the home are more varied [3, 36, 73, 78, 123, 127]. Thus, across all vignettes, we kept the device located in the indoor common space (where bystanders are most likely to be subject to data collection, and have varied opinions about the device's placement). However, in the exit survey we asked participants about the acceptability of different data retention policies, and the relative importance of device location in deciding the acceptability of data flows.

As noted in §2.2, prior research on relationships and power dynamics in smart homes, and their effects on privacy, have most commonly been studied in the context of families. In this study, when selecting the Situations, we focused instead on common smart home scenarios with different types of power dynamics between individuals who are *not* family. Specifically, the shared housing Situation evokes no obvious power dynamics, with usually relatively equal rights between two housemates, where both have contractual and financial obligations towards the landlord or property manager but not towards each other.[1] The relationship between a host and a guest staying at a friend's house overnight presumably also involves relatively equal power dynamics most of the time, but in the moment, the guest is dependent on the host's hospitality. The relationship between an Airbnb host and a guest renting their home potentially has somewhat unbalanced power dynamics, in that ownership of the home is in focus, and the parties have specific contractual and (for the guest) financial obligations towards each other, but no personal loyalties. Power dynamics are most obvious—and likely most imbalanced—in the relationship between a domestic worker and their employer, where there are mutual contractual obligations and a financial obligation on the part of the employer, the device owner is the boss *per se*, and the domestic worker's livelihood is dependent on the relationship.

In selecting Devices,[2] we considered adoption rates, data formats they collect, and relative levels of users' concerns with those devices according to prior studies [e.g. 3, 36, 41, 78, 125, 127]. To avoid confounds between smart cameras and smart door locks that have embedded cameras, we clarified in the device descriptions that, for the purpose of the survey, we consider smart locks that are *not* integrated with a camera (see Appendix B).

We eliminated some parameter values that were not logically compatible, based on observation of real-world practices and domain knowledge. For example, there is no point in sharing data with a government entity to troubleshoot or improve a device's performance, and it is unlikely for a smart door lock to go undisclosed, at least implicitly, as anyone can see it has some smart features as they use the door to enter the home. Three researchers reviewed and discussed all the value combinations for each pair of parameters. Because of such compatibility differences, participants were shown a different number of vignettes, depending on the Device and Situation they were assigned to. This affected the length of the survey. Most notably, surveys about cameras were the longest, as they collect data in three formats, followed by smart speakers (two formats), and then smart door locks (one format).

Exit Survey. The exit survey (see Appendix C) included questions about, for instance, relative influence of different factors on participants' acceptablity judgments. We also asked about participants' encounters with smart internet-connected devices, how comfortable they are interacting with those devices, education or work experience in technical fields, privacy attitudes, prior experiences with privacy or security violations, and what privacy controls they would like bystanders to have over smart home devices.

3.2 Recruitment and Ethics

We deployed our survey in Qualtrics and recruited participants on the research platform Prolific. We obtained an IRB exemption from the lead author's institution before conducting the research. All participants gave informed consent. We recruited a sex-balanced sample of participants age 18+, currently residing in the US and fluent in English. Prolific provided information on participants' demographics and ownership of Internet-enabled products. Due to the differences in survey length described above, participants' median completion time was 14.8, 12.5, and 12.4 minutes for the smart camera, smart speaker, and smart door lock versions, respectively, and we paid \$4, \$3.75, and \$3.25 (aiming for \$15/hour).

Before running the main survey, we used the user testing service UserFeel to recruit 6 pilot participants to test survey comprehension and flow. We refined the survey wording based on their feedback.

An initial power analysis using G*power [48] indicated a total sample size of 241 participants being sufficient for our study.[3] Post-hoc analysis confirmed that we achieved a statistical power of 1.0 in all regression models with our eventual sample ($N = 761$).

3.3 Analysis

3.3.1 Quantitative Analysis. To visualize how acceptance of information flows varies across Roles, Situations, and other parameters, we used heatmaps for compatible pairs of parameters (as explained above), following previous research on privacy judgments within smart homes and similar contexts [2, 19, 20].

We conducted inferential statistical analysis to systematically examine the relative impact of contextual parameters and participant characteristics on privacy acceptability judgments. Using the Variance Inflation Factor (VIF) analysis, we confirmed the absence of multicollinearity among the predictor variables [91, 122].

Using visual inspection and the Kolmogorov-Smirnov test [85], we found that our data is not normally distributed. Therefore, we chose to employ the Cumulative Link Mixed Model (CLMM) [34, 116]. The CLMM is particularly suited for handling non-normally distributed ordinal dependent variables and incorporates both fixed and random effects to accommodate the non-independence of observations within groups or subjects. We applied Bonferroni correction [104] to p-values in all models to account for multiple comparisons. To choose the optimal model with control variables, we first ran a CLMM regression with all contextual parameters and control variables (personal characteristics, like demographics and prior experiences and background) and then used a step-wise elimination process to remove the control variables that did not improve the model's explanatory power. Further CLMM regression analyses explored the impact of interaction effects.

3.3.2 Qualitative Analysis. To analyze the open-ended responses about desired privacy controls, we used thematic analysis. Two of the authors independently developed initial codebooks, then discussed and merged them. They coded the data using the final codebook, applying one or multiple codes, calculated agreement rates, and eventually reached a 100% agreement rate after discussing and resolving all disagreements. We discarded six invalid responses, where both coders suspected that the answer was copied from Internet sources or produced using generative AI (based on unusual length, phrasing, and structure of the response).

To compare the differences in code occurrences across Roles, Situations, and Device types, we used a pairwise Chi-Square test for codes with more than 5 occurrences, and Fisher's exact test for codes with 5 or less occurrences. We again applied Bonferroni correction [104] to account for multiple comparisons.

[1] We used gender-neutral names (Jackie and Adrian) in the shared housing scenarios to avoid potential impacts of gender stereotypes on participants' responses.

[2] As Device is the technical means by which the data is *captured*, we do not align it with a CI parameter, as CI describes elements of *sharing*.

[3] We ran a linear multiple regression model with an effect size of 0.15, α err probability of 0.05, β err probability of 0.90 and 35 total predictors.

3.4 Limitations

Our survey focused on some common parameters and situations that presented interesting tradeoffs, as suggested by prior research or common sense. However, to maintain a reasonable number of parameters for quantitative analysis, we had to exclude or fix some possible dimensions. Future research can complement our work by examining additional contextual factors, such as data senders, placement of devices, and other transmission principles. Research could also compare additional situations involving bystanders, including use of smart home devices at home vs. institutions like student housing or assisted living facilities, or use of IoT devices at work in an office, or could dive into more nuanced detail, for example by comparing specific types of domestic workers (e.g. caregivers for different groups such as children, elderly or disabled adults, or pets; non-care workers such as regular housecleaners or occasional home maintenance workers; or outdoor workers like gardeners). Such research may consider additional elements of the relationships between device owners and bystanders, such as preexisting trust, contractual obligations, short vs. long-term contact, etc.

Similarly, future work may assess the impact of the usability and complexity of privacy disclosures on acceptability judgments. For purposes of the study, we presented participants with (relatively) straightforward information about data flows, but in reality, bystanders and even owners may not have access to such information, or it may be more difficult to understand.

As with all vignette studies, we were asking participants for opinions about imaginary scenarios with certain assumptions and defined parameters, and their self-reported responses may differ from what they would have thought in real life, in naturally more complex or uncertain situations. Future research may compare our findings on normative privacy judgments with actual decisions or behaviors of bystanders and device owners in real life. While observational studies in realistic settings would have greater ecological validity, they would inevitably suffer from lower internal validity due to researchers' reduced control over contextual parameters. Thus, our internally valid study using hypothetical vignettes offers an important contribution that can complement future field studies.

Using second-person scenarios that asked participants to imagine themselves in a specific role allowed us to begin exploring the degree to which apparent norms might actually be commonly held, vs. whether there might be disconnects between norms assumed by people in different roles. However, although it is common in CI vignette studies [e.g. 2, 19, 58, 89, 119, 124], using "you" may encourage participants to consider their personal preferences, not just (their perceptions of) societal norms. More generally, surveys of individuals inherently provide only an incomplete view of norms, which are an abstract property of groups—but will not be construed in the same way by every individual in the group. On the other hand, as noted by Shvartzshnaider et al. [105], vignette-based surveys can at least establish an "implicit consensus" about contextual privacy norms as viewed by a majority of survey-takers.

4 Results

Next, we describe the participant pool and insights from the data analysis that answer our research questions. If we do not specify that a finding is specific to participants in one Role or the other, it means the finding is about all participants.

4.1 Participants

In total, we recruited 802 participants, but excluded 41 responses due to data quality issues (failing at least one attention check and/or finishing the survey too fast, defined as 1 standard deviation below the mean). We report the remaining 761 participants' responses, including 33,674 ratings of parameter combinations in the vignettes.

Participants' ages range from 18 to 72 y.o. (mean=38). The sample is balanced in terms of gender. The majority of participants are white (74%), employed full-time (72%), and are not students (86%); a plurality have undergraduate degrees (42%). Slightly over a quarter (27%) said they have education or work experience in a technical field (such as computer science, software engineering, or app development). A majority (72%) said that, in general, they are comfortable interacting with smart internet-connected devices. This is in line with market research results [21]. Finally, 39% said they had experienced some kind of information privacy or security violation or incident in the past. Table 2 in Appendix D summarizes participants' demographics and experiences.

4.2 Findings

4.2.1 ***Context-Dependent Privacy Judgments.***

To answer **RQ1**, we visualize participants' responses across the vignettes using the heatmaps in Figures 1, 2, and 3 (larger versions are in Appendix G). These heatmaps illustrate patterns in levels of acceptance across various pairs of contextual parameters, between participants assigned to different Situations and Roles.

Regarding Purposes, sharing device data for ensuring the safety of the people in the home and assisting in investigating a crime is viewed as acceptable across many vignettes (Fig. 1, 2, 3), while providing customized service/product recommendations is viewed as unacceptable in all vignettes. Enforcing house rules and troubleshooting the device are viewed as acceptable only for door locks in the domestic work Situation, by participants in both Roles (Fig. 2). Interestingly, while participants playing the Role of a guest staying at a friend's house overnight found it acceptable to share their smart door lock data for enforcing house rules and troubleshooting, participants playing the Role of the host in the same Situation did not find it acceptable. A similar surprising result is found for troubleshooting smart door locks in the Airbnb Situation.

In terms of Recipients, on average, participants found it unacceptable to share bystanders' smart home data with anyone other than the device owner, with a few exceptions when ensuring safety or investigating a crime (Fig. 3). Compared to the views of participants playing bystanders, participants who played the Role of device owners saw it as acceptable to share data with the device owners for a wider variety of Purposes (including for sharing a memory and monitoring work, which are otherwise viewed as unacceptable Purposes by both Roles in all other vignettes), especially in the employment and Airbnb Situations (Fig. 3). For the participants who were assigned a bystander Role, besides ensuring safety and assisting in investigating a crime, sharing the data with device owners and the manufacturer's employees was acceptable only for troubleshooting or improving the device's performance (Fig. 3).

We also compared the acceptance scores regarding different data senders and retention periods from the exit survey. Most participants (across both Roles) thought it unacceptable for device manufacturers (68%) or the device itself (62%) to share bystanders' data. However, 25% of participants in the bystander Role vs. 44% of participants in the device owner Role thought it acceptable for device owners to share bystanders' data (Chi-square test, $p<0.0001$). Three quarters of the participants in both Roles thought it acceptable for bystanders' data not to be stored at all. However, participants in the owner Role found other retention periods more acceptable than participants in the bystander Role, including deleting bystanders' data immediately after the purpose of use is achieved (77% vs 67%, $p = 0.0027$), deleting data after 1 month (64% vs. 53%, $p = 0.0048$), keeping data until bystanders request deletion (49% vs. 39%, $p = 0.0055$), and keeping it indefinitely (10% vs. 5%, $p = 0.0073$).

4.2.2 ***Quantitative Variation in Factors Affecting Privacy Judgments.*** Here we answer **RQ2**, aiming to understand what factors affect privacy acceptability judgments the most.

Recipients, Purposes, Device, and Data Format Have Significant Impact. First, we constructed a model in which we included only the contextual parameters, without demographics and other controls (see Model 1 in Table 6 in Appendix F).

We found that all Recipients and Purposes of sharing have a significant impact on acceptance levels. For example, in terms of odds ratios, compared to the device owner, the device owner's contacts are 82% less acceptable as Recipients, followed by third-party company employees (77% less acceptable), and government entities and the device manufacturer's employees (both 59% less acceptable). Monitoring work is 82% less acceptable than ensuring the safety of people in the home, followed by providing customized recommendations (79% less acceptable), sharing a memory (75% less acceptable), enforcing house rules (68% less acceptable), and troubleshooting or improving device performance (50% less acceptable). Assisting in investigating a crime is the only Purpose more acceptable than ensuring safety (77% more acceptable). Smart speakers are 43% less acceptable and smart door locks were 75% more acceptable than smart cameras. Sharing device logs/history of interactions is viewed as 19% more acceptable than audio recordings, with no significant difference in acceptance between video and audio recordings.

All of these coefficients were also significant (with slight variations in magnitude) in Models 2–5 described below, except for smart door locks, due to the higher Bonferroni-corrected p-values.

The insights from the regression analysis broadly align with participants' self-report about the importance of factors (Table 5 in Appendix F), with Recipients, Purposes of sharing, and Data formats having the strongest impact. Role, Situation, and level of Transparency did not significantly influence acceptance levels in regressions, except in interaction with the more influential factors.

Interaction Effects Reveal the Nuances. We also tested the interaction effects between Recipients, Purposes of sharing, and Situations (Table 7 in Appendix F). While some significant interaction effects were more predictable from the effects of individual variables, others are more surprising, shedding light on the contextual nuances of privacy judgments. Although when considered alone, all Recipients were seen as less acceptable compared to the device owner, certain interactions between Recipients and Purposes of sharing (Model 3) or Situations (Model 4) were seen as more acceptable. For example, although compared to the device owners, government entities are typically not favorable data Recipients, sharing bystanders' data with the government to assist in investigating a crime or in an Airbnb Situation on average was seen as acceptable. Similarly, many participants thought that sharing data with manufacturers' and third party companies' employees is usually not acceptable, but made exceptions for device troubleshooting, or when it happened in an Airbnb Situation. One potential explanation is the congruence between the Recipients and Purposes, where government involvement in investigating a crime or companies' involvement in troubleshooting the device are viewed as beneficial or even necessary. In turn, a potential explanation for the surprising interactions between Recipients and Situations might be that sharing information with an impersonal entity or organization (rather than an individual person) seems more acceptable in a Situation that doesn't imply a personal relationship between the device owner and the bystander.

In Model 5, although enforcing house rules had negative coefficients when considered alone, participants found it a quite acceptable Purpose when house rules are enforced in the domestic work Situation. Additionally, in Model 4, data flows in the domestic work Situation were viewed as 166% more acceptable than in the shared housing Situation. Both of these effects could be explained in part by power dynamics between employer and employee (see §5.1).

Comfort with IoT, Education Level, and Privacy Attitudes Affect Privacy Judgments. To answer **RQ3**, we added control variables, including demographics, prior experiences in the relevant smart home situations, and attitudes about privacy of self and others to the regression model with the individual contextual factors (see Model 2 in Table 6 in Appendix F). We found that higher general comfort with IoT devices, and having a high school diploma as the highest education level achieved, are associated with higher levels of acceptance of data flows. On the other hand, level of privacy concern about collection of users' own data (IUIPC sub-scale on data collection) is associated with lower acceptance—though concern about the privacy of *others* did not have a significant effect.

4.2.3 ***Insights about Desired Controls.*** To answer **RQ4**, we analyzed the open-ended responses about privacy controls participants for bystanders' data in smart homes. To answer **RQ5**, we ran statistical tests on the differences in code occurrences across Devices, Roles, and Situations. Our codebook and example quotes are summarized in Table 3, and occurrence counts and statistical results are summarized in Table 4, both in Appendix E.

The analysis revealed different strategies for managing bystanders' data privacy that vary in the level of control that bystanders have over their information. For example, the responses ranged from bystanders not having any privacy controls at all, through basic transparency, to binary choices, or more nuanced decisions. At the extreme, 9% of participants said that bystanders need *no privacy controls*. This view was twice as common among participants in the device owner Role compared to the bystander Role (12% vs. 6%, $p = 0.0313$). In particular, many participants noted that a smart door lock does not need much by way of privacy controls as long as it's not integrated with a camera (which it wasn't, in our scenarios).

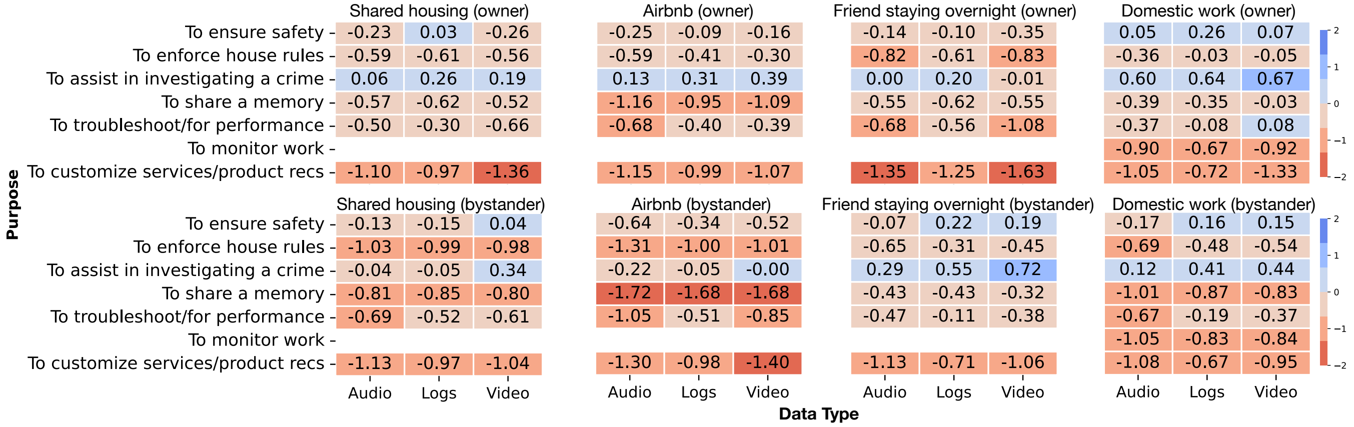

Figure 1: Average acceptance scores for information flows across Data formats × Purpose of sharing pairs.

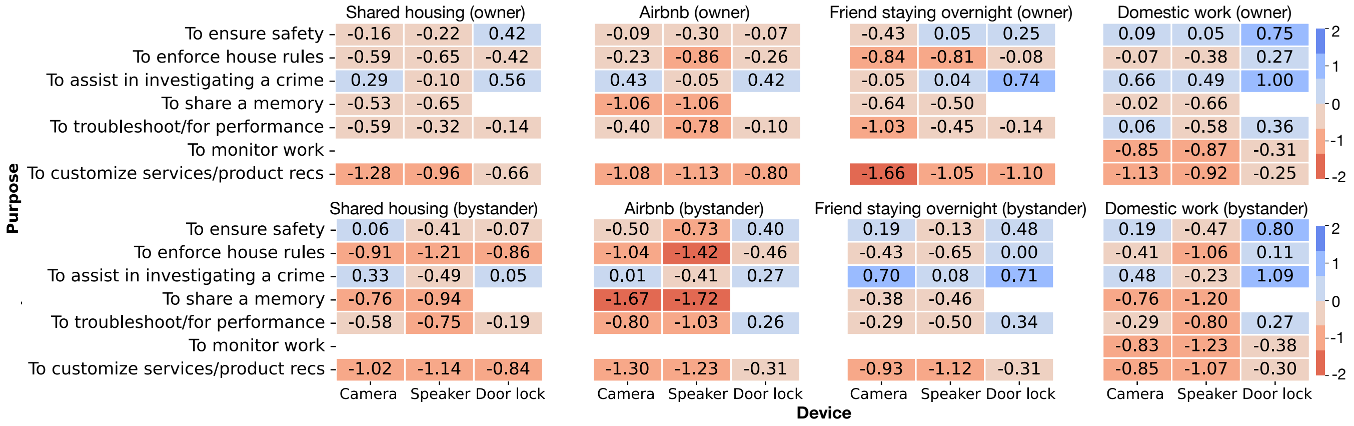

Figure 2: Average acceptance scores for information flows across Device type × Purpose of sharing pairs.

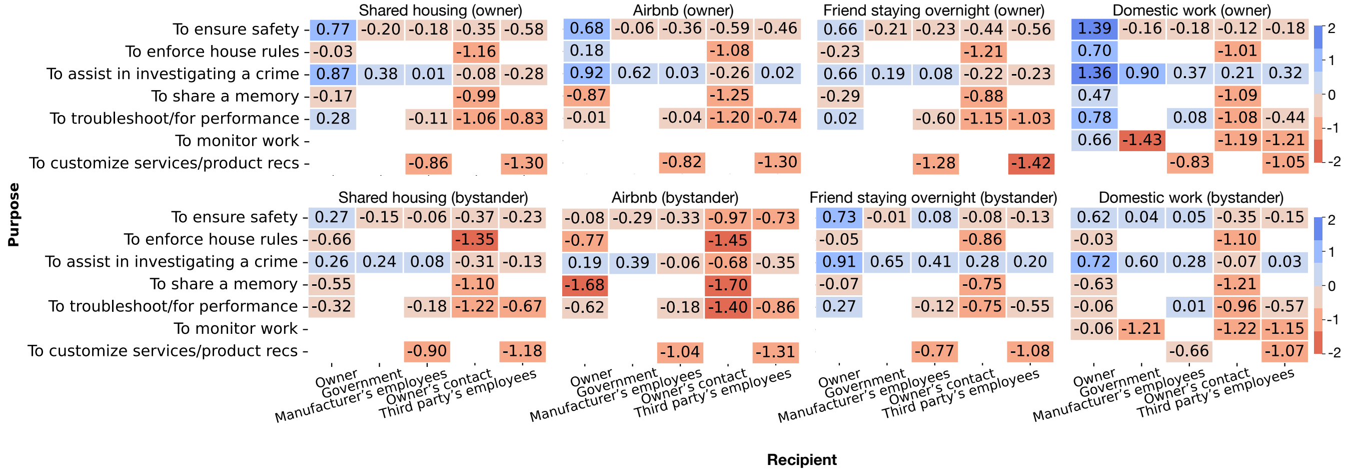

Figure 3: Average acceptance scores for information flows across Recipient × Purpose of sharing pairs.

The most common theme was the necessity of *disclosure* of the device's presence and main data practices, e.g. via verbal or written notices (21%). This was mentioned almost twice as often for smart cameras as for speakers (29% vs. 15%, $p = 0.0347$), possibly because a camera is considered to be more invasive than a speaker, as implied by our regression analysis of acceptance levels (Model 1 in Table 6).

Another form of alerting bystanders that a device is on or recording is the device's own *feedback*, for example lights or sounds. Feedback was suggested by 0.8% of participants, all in a bystander Role.

One step beyond basic disclosure is to obtain *consent* or permission from bystanders for collecting or sharing their data (6%). As well as one-sided consent, 1% of participants thought device owners and bystanders should have a two-way *discussion* or negotiation about device configuration and data practices. As another transparency mechanism, 7% of participants suggested bystanders should be able to *view their data*, for example, in a dashboard or guest mode/account, or by requesting a copy of their data.

The second most popular type of control mechanism, after disclosure, were various means to *opt out* of data collection, for example by turning off, unplugging, muting, or physically covering the device, or avoiding creating a voice profile for bystanders, to prevent devices from recording and recognizing their voices. Opt-outs were suggested by 17% of participants, though less commonly for locks than for speakers (7% vs. 24%, $p = .0001$). Using a device that is *not Internet-connected* and processes data locally (0.7%) or is *analog* and does not generate digital data at all (0.8%) were other suggested ways to prevent excessive data collection and sharing.

Other proposed controls were more granular and allowed for nuanced data management strategies. Among those, it was most common to want to *limit data* that is collected or shared (13%), e.g. by choosing what specific data types are allowed to be collected, or in what format. Such suggestions were especially common for speakers, compared to locks and cameras (21% vs. 10% and 7%, $p = 0.0114$ and $p < .0001$), because participants did not want smart speakers to record their private conversations. If data were already collected, participants wanted to at least *obfuscate* their identity or information (1%), for example by blurring faces or changing voices.

Participants also wanted to *limit access* to data (13%) by choosing potential recipients. Preventing sharing of bystanders' data with a third party was especially common: *"I don't love the company that made the speaker having access to it, I really don't like a third party being involved, and the idea of the government having access to it for any reason is pretty horrifying."* - P194. Interestingly, 10 of those participants (across both Roles) said that sharing with device owners should nevertheless be allowed, as they should be in ultimate control of their home and devices.

Many participants wanted to *limit storage* of bystanders' data by preventing retention or choosing for how long the data is stored before being automatically deleted (9%), or to be able to proactively *delete the data* directly through a dashboard or by requesting that the owner do it (6%). Deleting after one month or after the bystander has left the house was often viewed as acceptable. Participants in the device owner Role wanted to make sure that no damage to the property or other violation of house rules occurred before deleting bystanders' data: *"I'd like them to be able to delete their data after 3 days of leaving the home. I would want to check the footage and make sure nothing was broken or damaged, then delete it."* - P505.

Limiting purposes for which bystanders' data is collected, used, or shared is another approach mentioned by 3% of participants. For example, participants were willing to share only if the bystanders' data was required for an important reason, such as ensuring safety, preventing crime, assisting in criminal investigations, and in case of emergencies. Some (2%) wanted to *limit when* bystanders' data is collected, e.g., to avoid the times when the bystanders are not working (in the domestic work Situation), or only collect during certain hours of the day: *"Maybe something that is audio [recording] only from like midnight to 6am or something like that?"* - P504.

Finally, 7% of participants wanted to *limit the locations* where the devices are placed, for example, choosing only common spaces and avoiding private spaces like bathrooms and bedrooms, avoiding any indoor locations at all, or limiting the locations to owner's own rooms, avoiding common areas. Interestingly, while limiting locations seems largely a moot point for smart locks, location was mentioned similarly infrequently for speakers, and both speakers and locks were both disproportionately less likely than smart cameras to prompt location limitations (15% vs. 3% and 2%, $p < 0.0001$).

We described above how participants suggested exceptions for certain limitations, for example, to always allow access to the data for the device owner or in case of emergency. Other exceptions (mentioned only by participants in the device owner Role) included specifying that bystanders could be provided with transparency (e.g. disclosure or ability to view data) but not any active controls (e.g. deleting data or configuring settings) (1%), and specifying that bystanders could have access to or management rights over their own data but not the device owner's data (0.5%). In general, exceptions regarding bystanders' privacy controls were mentioned by participants in the device owner Role more often than by participants in the bystander Role (10% vs. 3%, $p = 0.0002$), which indicates a recognition of power imbalance, and a device owner's greater desire for ultimate control over data practices.

Meanwhile, 4% of participants, predominantly among those in the device owner Role (7% vs. 2%, $p = 0.0026$, said they would like bystanders and device owners to have *equal privacy control*, and 1% mentioned that their decision about the appropriate level of privacy controls would depend on the relationship and level of *trust* between the bystander and device owner or other data recipients.

In addition to privacy controls, several participants mentioned a desire for data *security* (2%), including *encryption* of bystanders' data (0.3%) or strong *passwords* for their smart home accounts (0.3%).

Some of the suggested privacy "controls" were not controls on the device at all, nor even suggestions about the owner's behavior, but rather required the bystanders themselves to change their behavior. For example, a bystander might prevent data collection by simply *avoiding using the device* or interacting with it (mentioned by 3% of participants). Sometimes not using a device like a smart camera is only possible by not entering a home that has one at all: *"I would not stay in a residence that had a smart device that collects data about the people in the home. Absolutely not."* - P269. A less common strategy for avoiding data collection is to *change behavior* when one is near a device (0.8%), for example avoiding sensitive conversations.

5 Discussion and Future Work

In this section, we discuss implications of our findings; recommendations for software teams and policy makers; and directions for future work. We note that, while the possibility for transparency and control should be conditions of smart home data sharing (reflecting transmission principles in CI terms), privacy-respecting design and policy require attention to broader aspects of context to reflect privacy norms held by both owners and bystanders.

5.1 Power Dynamics in Smart Homes

Our descriptive (§4.2.1) and qualitative analyses (§4.2.3) showed that participants playing the Role of device owners tended to have less privacy-protective views on handling of bystanders' data than those playing a bystander Role. For instance, they more often viewed as acceptable storing bystanders' data for longer periods of time, providing no bystander privacy controls at all, or restricting such controls. Such misalignment is problematic given that device owners have primary control over data flows—and participants in the owner Role were also less likely to suggest strong controls for bystanders. Device owners making decisions about bystanders' data without consulting them would likely choose less restrictive privacy settings (e.g. longer data retention) and feel more comfortable accessing or sharing bystanders' data. The misalignment could also exacerbate existing unbalanced power dynamics. Prior work on Contextual Integrity acknowledges the importance of such implications in evaluating data practices, e.g. in the CI decision heuristic's reference to moral and political factors such as effects on power structures and power relations [69, 92].

On the other hand, although when various factors were taken into consideration in regression analysis, differences between Roles were not statistically significant (§4.2.2), heatmaps of Likert scale responses (§4.2.1) reveal that there are cases where participants in a bystander Role found it acceptable to share their data, e.g. for enforcing house rules, troubleshooting, ensuring safety or investigating a crime, especially in the Situations involving being in other people's houses, whereas participants in a device owner Role did not always find it acceptable. This may also reflect the impact of power dynamics, where bystanders are dependent on the hosts' hospitality or generosity, and may feel obliged to accept sharing of their data as part of a financial arrangement. Prior qualitative work has also found the tendency of domestic workers to prioritize employers' interests over personal privacy concerns [11, 26]. Short-term rental guests may feel they don't have much choice about accepting hosts' devices [78, 125]—but hosts, in their turn, have financial incentives to provide a comfortable experience [96].

Future research can further tease out how power dynamics interact with the formation and collective acceptance—or imbalanced acceptance—of bystander privacy norms [see 98]. Future work should also explore ways to reduce the impact of power dynamics between device owners and bystanders in negotiating privacy practices and configuring settings of smart home devices.

5.2 Recommendations for Future Research

Our work contributes empirical evidence about bystanders as smart home data subjects and compares privacy judgments across a variety of contextual factors. Interactions between factors reveal some additional nuances (see §4.2.2). These findings demonstrate the value of paying attention not only to contextual factors in isolation, but also to their complex interplay.

However, the fact that differences in privacy judgments by Situations and Transparency levels were not statistically significant, except some interaction effects, suggests that norms about information sharing are *relatively* consistent across various types of relationships between bystanders and device owners, and regardless of whether sharing is disclosed or in how much detail. This presents an interesting contrast with prior work. For example, Cobb et al. [36] found significant differences by situation/relationship in dislike vs. appreciation for devices; however, they did not compare the impact of different factors on privacy views specifically. Most similar to our study, Chiang et al. [32] found that relationship between bystander and owner, and to a lesser degree device and data type, affected how consent processes impacted participants' views on acceptability of data collection (though they did not test the interplay of factors as in our full factorial vignette design; see §2.2.5). Further study is needed to determine whether the difference was driven by the dominant effects of data recipients and purposes in our study (which were not analyzed by Chiang et al. [32]), whether aspects of disclosure and consent are less important in determining acceptability of data sharing than of collection, or some other factors. Interestingly, although on average our participants in the bystander Role showed lower acceptance of data flows than those in the device owner Role, the differences were not statistically significant. The qualitative responses about controls were also largely similar between the Roles, with differences being mainly a matter of prevalence rather than kind. Thus, our findings suggest relative alignment of privacy norms about sharing of bystander data between bystanders and device owners. This finding contrasts with those of Alshehri et al. [15, 16], Thakkar et al. [117], and Mare et al. [78], who found more discrepancies between the views of bystanders and device owners, or participants playing those roles. In Zhou et al.'s [135] experiment with a prototype negotiation aid, participants assigned to owner vs. bystander roles often started with divergent views—but both roles were often flexible and willing to compromise. None of these studies compared the impact of role with other contextual factors on the aspects they studied, and it may be that (as in our study) a detailed quantitative analysis might show any differences to be less significant than other variables. However, the contrast is intriguing, and future work is called to further investigate the interplay of (potentially) divergent *preferences and expectations* with (potentially) more unified *sharing norms* in the shaping of *negotiation behaviors* with regard to bystander data, and how each aspect interacts with other contextual parameters.

In the cases noted above, the varied studies used similar enough values for the contextual parameters that we can draw comparisons. However, the values were not identical even for those cases, and in many other cases, the values tested were quite different (not just in phrasing but in intent). This makes it difficult to directly compare their coefficients of impact. Future work may conduct a meta-analysis and propose a mapping of parameter values for comparing insights across different smart home privacy studies.

5.3 Practical Recommendations for Smart Home Product Teams and Practitioners

Current privacy mechanisms in smart home devices are geared towards primary users, and do not take into consideration bystanders' privacy perspective and concerns. To address this gap, it is important for software teams to engage in user research with secondary users (who do not have the same access/control as primary users) and other bystanders (e.g. domestic workers or visitors), to assess privacy implications for broader groups of impacted stakeholders. However, the fact that participants' privacy views and preferred privacy controls did not differ much between the Situations we explored, modulo a few nuanced interactions, suggests that these situations do not require entirely different bystander privacy solutions. Rather, they require solutions to be flexible enough to account for some nuances. The mechanisms we suggest below are therefore mostly applicable to any bystander situation/relationship to the owner, but we note some cases where specific measures might make the mechanisms accessible to bystanders in a particular situation, or more likely to be used in that situation.

5.3.1 ***Disclosure and Transparency for Bystanders.*** Currently, smart home consent and transparency mechanisms (such as privacy policies or data safety labels in companion apps) rely on directly interacting with the devices or their companion apps. Thus, transparency mechanisms available to bystanders are limited to device feedback (e.g. LED indicators and sounds). However, only a few of our participants mentioned device feedback as a desired bystander privacy control (see §4.2.3)—possibly because it doesn't actually allow control *per se*. Moreover, prior work has shown that people often misunderstand the meaning of device feedback [e.g. 7, 38].

Prior to making decisions about specific controls, our participants pointed out that bystanders need to know that the device is present; where it is located; what data it collects, uses, or shares; how long and where data is stored; and whether bystanders *can* have any control over it (e.g. to request deletion). Disclosure of these specifics is therefore a critical step in granting bystanders control over their data, as suggested by prior work [e.g. 26, 31, 32, 36, 86]. However, ensuring transparency should not be viewed as the sole responsibility or legal obligation of device owners, as they are "amateur controllers" [60, 112, 121] and may lack knowledge about smart home data flows themselves. Manufacturers should lead in making such information available and clear for bystanders, rather than making it the *de facto* responsibility of device owners. For example, smart home devices could have a QR code bystanders could scan to access disclosures, ideally in a concise, standardized format like a privacy "nutrition label" [see 30, 44, 49, 79–81]. It would be especially helpful to outline data practices and protections for *bystanders'* data, including any control mechanisms they can use.

Free access to information about data practices could help mitigate information asymmetry [6, 24, 35] between device owners and bystanders, which can be exacerbated in relationships with uneven power dynamics. Manufacturers could encourage device owners to have a printed version of privacy nutrition labels on hand, in case bystanders don't have a smartphone, don't know how to scan a QR code, or can't reach it. However, as printed disclosures would need to be regularly updated, they might be most useful in situations that already involve document exchange (e.g. rental agreements, domestic work contracts).

Prior work has also suggested developing capabilities for smart speakers (called Skills) to directly answer questions about the device's data practices [70, 86, 113, 117, 130]. Meng et al. [86] recommended leveraging existing social norms for introducing humans (e.g. the owner introduces the device by name, and it gives a quick overview of its capabilities, including mute modes). We suggest this approach can be further extended, offering a brief overview of its data practices and asking for guests' consent to collect data.

Other entities (such as short-term rental companies, domestic work agencies, professional associations, etc.) can help facilitate disclosures and provide guidelines; such guidelines are currently rare exceptions rather than industry standards [96]. For example, Airbnb provides guidance to its users, including requiring disclosure of cameras [8, 9]—but hosts are *not required* (only encouraged), to disclose other devices like smart speakers and smart thermostats [9]. However, our study suggests that guests would appreciate disclosure of smart speakers. Moreover, Airbnb policies do not require disclosing specific data practices [8]; greater transparency in that regard could further improve Airbnb's (and other platforms') efforts to resolve privacy tensions between guests and hosts.

5.3.2 ***Opt-Outs and Settings for Bystanders.*** While disclosures provide transparency, they don't provide *control* over data flows. Currently, bystanders' controls are typically limited to physical controls (e.g. mute or on/off buttons, or simply unplugging the device [36]). While the ability to opt out of data collection was the second most frequently desired privacy control, such binary opt-out strategies may compromise the utility of the device, thereby depriving bystanders (and in some cases primary users) of potential benefits [16, 36, 79, 118, 125]. Thus, participants suggested more nuanced ways for bystanders to view and control data flows, such as dashboards, privacy settings, or guest accounts/profiles. While guest profiles [e.g. 52, 97, 128, 132] could be more useful for frequent visitors (like family members, domestic workers), physical dashboards [e.g. 39, 46, 117, 128] would be more convenient for incidental users and temporary visitors. As our participants emphasized, such mechanisms should allow managing bystanders' data only, without giving bystanders control of owners' data.

5.3.3 ***Other Bystander Privacy Features.*** The usability flaws of existing transparency and control mechanisms for primary users are well-documented, as is the problem of privacy decision fatigue [e.g., 99, 120] [overviews in 5, 14]. New disclosures, consent mechanisms, and controls for both bystanders and primary users should be designed around usability principles [4, 37, 101, 102], and tested for usability [56]. But at the same time, smart home devices should also incorporate designs that provide bystander privacy by default [overview in 100].

Our participants suggested features for limiting data collection (e.g. not capturing private conversations, setting windows of time when collection is permitted) and obfuscating bystanders' voices and faces. Machine learning techniques can distinguish primary users from bystanders to facilitate such protections, even without bystanders having direct access to the system [see 11, 36, 70, 78, 115, 130]. Current implementations include voice profiles for smart speakers [17, 53], where the device "ignores" voices not linked to a profile. However, such features are less common in other devices, such as smart cameras, and represent a gap in available controls. Proposed frameworks that can infer contextual parameters and implement access permissions appropriate for the particular situation [e.g. 103] merit exploration as well [overview: 59]. However, as noted in prior research [e.g. 11, 36, 114, 115, 118], while addressing one type of privacy risk, adding recognition features may introduce new ones, for both bystanders and primary users. Therefore, future work should carefully assess privacy risks of any such systems.

Our participants preferred shorter data retention periods, especially those in the bystander Role. To facilitate timely deletion of guests' data, Mare et al. [78] suggest that Airbnb or other short-term rental platforms could develop an integration with the smart home devices' platforms, to allow hosts to set up and revoke device access. We note that such an API could also allow automatic purging of guests' information, for example after allowing a week for hosts to notice any rental policy violation, as suggested by our participants. In general, smart home interfaces could nudge owners to select short retention periods for the sake of bystanders.

Our participants also found the use of logs / history of interactions more acceptable than audio or video recordings. This suggests that device manufacturers should consider storing and using logs and history of interactions instead of audio and video recordings for delivering services whenever possible, to better meet privacy norms. We suggest using principles of data minimization and least privilege [e.g. 11, 78, 118] to limit storage (e.g. to only logs) and limit access to only specific data points about bystanders that are required to fulfill a particular goal, e.g. only sharing noise levels with the house owner to enforce house rules.

5.3.4 ***Supporting Negotiation and Privacy-Preserving Norms.*** Many of our participants mentioned that their preferred privacy protections would depend on the relationships and levels of trust between bystanders and device owners. To translate our findings about bystander privacy norms into practice, manufacturers could design interventions that scaffold privacy-preserving norms for secondary users' and bystanders' data (as suggested by Zeng and Roesner [132]). For instance, they could incorporate discussion guides about data practices in the device set-up interface [see 26], or nudge owners to consider privacy implications for bystanders and discuss it with them [see 3, 97, 107], or ask whether they have bystanders' explicit consent to view data about them [see 114, 132].

A few participants were interested in negotiation about privacy controls. Prior work has explored negotiation between bystanders and device owners [16, 36, 130, 135], including in Airbnb [96, 125] and domestic work situations [3, 12], and proposed tools to aid such discussions [15, 82, 135]. Wang et al. [125] found that Airbnb guests preferred to negotiate privacy with hosts directly during booking, and suggested that explicit support for such negotiation be integrated into platforms. As we noted in §5.2, the relative alignment of acceptability judgments between bystander and owner Roles in our study suggests that supported negotiations could be successful at reaching agreement, and are unlikely to instigate serious conflicts.

5.4 Policy Recommendations

Currently, privacy laws largely focus on protecting rights of primary users, and provide no practical ways for bystanders to exercise their privacy rights. There is a need to regulate the use and privacy protection of bystanders' data as well. Understanding social norms regarding flows of bystanders' data collected in smart homes supports development of laws and regulations aligned with both device owners' and bystanders' privacy expectations and norms (see §4.2.1). In particular, our participants found sharing of bystander data with government entities (including law enforcement) somewhat acceptable only for investigating crimes, and, in some cases, for ensuring safety. Therefore, policymakers need to better define legal conditions for obtaining smart home bystanders' data and boundaries on using it in legal cases, and update users' expectations about those boundaries through public communications.

Current consent mechanisms do not require device owners or device/service providers to obtain bystanders' consent. Policymakers should develop and enforce requirements for consent mechanisms that would allow bystanders (and not just owners) to provide informed consent in a variety of smart home situations. Extending transparency and disclosure standards to bystanders will necessitate examination of how implementation and stringent enforcement of standards for primary user vs. bystander privacy might differ, along with additional usability considerations. For example, policymakers should require manufacturers to provide clear, concise, and comprehensive privacy information that can be accessed by bystanders directly (e.g. via QR codes or on the product website), and disseminated by other entities (such as lodging rental companies, domestic work agencies, professional associations, etc.). Providing details such as those discussed in §5.3.1 can effectively empower bystanders' active control over their data and mitigate the pronounced information asymmetry and unbalanced power dynamics that currently exists between device owners and bystanders.

While transparency about data flows is the first step in informing privacy expectations and formation of privacy norms, policymakers and policy analysts working in smart home companies can use our findings for broader alignment of privacy regulations and policies with privacy norms about bystanders' data, beyond notice-and-consent. For instance, work like ours can provide a basis for operationalizing the notion of reasonable expectations of privacy, which is implicitly or explicitly incorporated in major European and U.S. privacy laws like GDPR [47] and CCPA [95]. Our insights about acceptability of Purposes and Recipients (and interaction effects between the two) can inform policymakers about expectations and norms regarding "legitimate interests" (GDPR, Art. 6(1)(f) and Art. 13) in using bystanders' data, and "legitimate purposes" that are "adequate and relevant" (GDPR, Art. 5), "reasonably expected" (CCPA, 1798.121), and "compatible with the context" (CCPA, 1798.100) in which IoT companies process bystanders' data, "taking into consideration the reasonable expectations of data subjects based on their relationship with the controller" (GDPR Recital 47).

6 Conclusion

Using Contextual Integrity theory, our study with 761 US participants examined variation in privacy judgments about bystanders' data in different smart home contexts, including situations like domestic work, shared housing, overnight stays, and Airbnb scenarios. Our findings reveal that the recipients and purposes of data sharing have the greatest impact on acceptance of bystander data flows. Participants were generally more comfortable with sharing interaction logs than audio or video data, and data from smart speakers was deemed less acceptable to share compared to data from smart cameras or smart door locks. Additionally, we observed nuanced interactions between recipients, purposes, and situations, and some notable differences between the privacy protections most preferred by participants in bystander vs. owner roles. Based on these insights, we recommend smart home privacy protections be designed with greater consideration for the privacy needs of bystanders.

Acknowledgments

This research was supported by the U.S. National Science Foundation (award CNS-2114229), the U.S. National Security Agency (contract H98230-18-D-0006), and the UK Engineering and Physical Sciences Research Council (grant EP/T026723/1).

We thank our colleagues Junghyun Choy and Franziska Roesner, participants at the 2022 Symposium on Applications of Contextual Integrity, and members of the Berkeley Lab for Usable and Experimental Security for comments on the study design, and reviewers for ACM CHI and PoPETS for feedback that helped to improve the paper.

Special thanks are due to Ruba Abu-Salma and Tess Despres for substantive contributions to the study design and data preparation.

References

[1] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the 15th USENIX Symposium on Usable Privacy and Security.* 451–466.

[2] Noura Abdi, Xiao Zhan, Kopo M Ramokapane, and Jose Such. 2021. Privacy norms for smart home personal assistants. In *Proceedings of the 2021 CHI conference on human factors in computing systems.* 1–14.

[3] Ruba Abu-Salma, Junghyun Choy, Alisa Frik, and Julia Bernd. 2024. 'They Didn't Buy Their Smart TV to Watch Me with the Kids': Comparing Nannies' and Parents' Privacy Threat Models for Smart Home Devices. *ACM Transactions on Computer-Human Interaction* (2024).

[4] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, et al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 1–41.

[5] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2022. Privacy and Behavioral Economics. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing.

[6] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The economics of privacy. *Journal of economic Literature* 54, 2 (2016), 442–492.

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

[8] Airbnb. 2024. Informing guests about security devices. https://www.airbnb.com/help/article/2914 Last accessed 9 September 2024.

[9] Airbnb. 2024. Use and disclosure of security cameras, recording devices, noise decibel monitors, and smart home devices. https://www.airbnb.com/help/article/3061 Last accessed 9 September 2024.

[10] Wael Albayaydh and Ivan Flechais. 2022. Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. In *ACM Conference on Human Factors in Computing Systems.*

[11] Wael Albayaydh and Ivan Flechais. 2023. Examining Power Dynamics and User Privacy in Smart Technology Use Among Jordanian Households. In *32nd USENIX Security Symposium.* USENIX Association, 4643–4659.

[12] Wael Albayaydh and Ivan Flechais. 2024. Co-designing a mobile app for bystander privacy protection in Jordanian smart homes: A step towards addressing a complex privacy landscape. (2024).

[13] Wael Albayaydh and Ivan Flechais. 2024. "Innovative Technologies or Invasive Technologies?": Exploring Design Challenges of Privacy Protection With Smart Home in Jordan. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–54.

[14] Majed Alshamari. 2016. A review of gaps between usability and security/privacy. *International Journal of Communications, Network and System Sciences* 9, 10 (2016), 413–429.

[15] Ahmed Alshehri, Eugin Pahk, Joseph Spielman, Jacob T Parker, Benjamin Gilbert, and Chuan Yue. 2023. Exploring the Negotiation Behaviors of Owners and Bystanders over Data Practices of Smart Home Devices. In *Proceedings of the CHI Conference on Human Factors in Computing Systems.* 1–27.

[16] Ahmed Alshehri, Joseph Spielman, Amiya Prasad, and Chuan Yue. 2022. Exploring the Privacy Concerns of Bystanders in Smart Homes from the Perspectives of Both Owners and Bystanders. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 99–119.

[17] Amazon. 2024. What is Alexa Voice ID? https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=GYCXKY2AB2QWZT2X

[18] Noah Apthorpe, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. 2020. You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships. *arXiv:2001.10608 [cs]* (July 2020). http://arxiv.org/abs/2001.10608

[19] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable, and Ubiquitous Technologies* 2, 2 (June 2018), 1–23.

[20] Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA. In *28th USENIX security symposium.* 123–140.

[21] Axios. 2019. How comfortable are US Internet users with with the idea of smart home devices? https://www.statista.com/statistics/794480/us-amazon-echo-google-home-installed-base/. Last accessed 11-October-2023.

[22] Gianmarco Baldini, Maarten Botterman, Ricardo Neisse, and Mariachiara Tallacchini. 2018. Ethical Design in the Internet of Things. *Science and Engineering Ethics* 24, 3 (01 June 2018), 905–925.

[23] Natã M Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. 2019. "what if?" predicting individual users' smart home privacy preferences and their changes. *Proceedings on Privacy Enhancing Technologies* (2019).

[24] Masooda Bashir, Carol Hayes, April D Lambert, and Jay P Kesan. 2015. Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology* 52, 1 (2015), 1–10.

[25] Sebastian Benthall, Seda Gürses, Helen Nissenbaum, et al. 2017. *Contextual integrity through the lens of computer science.* Now Publishers.

[26] Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships. In *Proceedings of the 18th Symposium on Usable Privacy and Security.* USENIX Association.

[27] Clara Berridge and Terrie Fox Wetle. 2020. Why older adults and their children disagree about in-home surveillance technology, sensors, and tracking. *The Gerontologist* 60, 5 (2020), 926–934.

[28] Gergely Biczók and Pern Hui Chia. 2013. Interdependent privacy: Let me share your data. In *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17.* Springer, 338–353.

[29] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2020. A Privacy-Centered System Model for Smart Connected Homes. *IEEE International Conference on Pervasive Computing and Communications Workshops* (2020), 1–4.

[30] Claire C Chen, Dillon Shu, Hamsini Ravishankar, Xinran Li, Yuvraj Agarwal, and Lorrie F. Cranor. 2024. Is a Trustmark and QR Code Enough? The Effect of IoT Security and Privacy Label Information Complexity on Consumer Comprehension and Behavior. In *Proceedings of the CHI Conference on Human Factors in Computing Systems.* Association for Computing Machinery.

[31] Chola Chhetri and Vivian Genaro Motti. 2022. Privacy concerns about smart home devices: a comparative analysis between non-users and users. *Human Factors in Cybersecurity* 53, 53 (2022).

[32] Yi-Shyuan Chiang, Omar Khan, Adam Bates, and Camille Cobb. 2024. More than just informed: The importance of consent facets in smart homes. In *Proceedings of the CHI Conference on Human Factors in Computing Systems.* 1–21.

[33] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the ACM Conference on Ubiquitous Computing.* 61–70.

[34] Rune Haubo B Christensen. 2015. A Tutorial on fitting Cumulative Link Models with the ordinal Package. Retrieved from www.cran.r-project.org/package=ordinal.

[35] Gavin Clarkson, Trond E Jacobsen, and Archer L Batcheller. 2007. Information asymmetry and information sharing. *Government Information Quarterly* 24, 4 (2007), 827–839.

[36] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I would have to evaluate their objections": Privacy Tensions Between Smart Home Device Owners and Incidental Users. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 54–75.

[37] Lorrie F. Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273.

[38] Andrea Cuadra, Hyein Baek, Deborah Estrin, Malte Jung, and Nicola Dell. 2022. On Inclusion: Video Analysis of Older Adult Interactions with a Multi-Modal Voice Assistant in a Public Setting. In *Proceedings of the International Conference on Information and Communication Technologies and Development.* 1–17.

[39] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Human-Computer Interaction Conference.* ACM, Article 74, 13 pages.

[40] Tamara Denning, Tadayoshi Kohno, and Henry M. Levy. 2013. Computer security and the modern home. *Commununications of the ACM* 56 (2013), 94–103.

[41] Tess Despres, Marcelino Ayala Constantino, Naomi Zacarias Lizola, Gerardo Sánchez Romero, Shijing He, Xiao Zhan, Noura Abdi, Ruba Abu-Salma, Jose Such, and Julia Bernd. 2024. "My Best Friend's Husband Sees and Knows Everything"': A Cross-Contextual and Cross-Country Approach to Understanding Smart Home Privacy. *Proceedings on Privacy Enhancing Technologies* 2024, 4 (2024).

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

[43] Nils Ehrenberg and Turkka Keinonen. 2021. The Technology Is Enemy for Me at the Moment: How Smart Home Technologies Assert Control Beyond Intent. In *ACM Conference on Human Factors in Computing Systems*. ACM.

[44] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *IEEE Symposium on Security and Privacy (SP)*. 771–788.

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

[46] Stephan Escher, Katrin Etzrodt, Benjamin Weller, Stefan Köpsell, and Thorsten Strufe. 2022. Transparency for Bystanders in IoT regarding audiovisual Recordings. In *IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events*. 649–654.

[47] European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[48] Franz Faul, Edgar Erdfelder, Axel Buchner, and Albert-Georg Lang. 2009. Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior research methods* 41, 4 (2009), 1149–1160.

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

[50] Janet Finch. 1987. The vignette technique in survey research. *Sociology* 21, 1 (1987), 105–114.

[51] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 2 (June 2019), 44:1–44:21.

[52] Christine Geeng and Franziska Roesner. 2019. Who's in Control? Interactions in Multi-User Smart Homes. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*. 1–13.

[53] Google. 2024. Link your voice to your Google Assistant device with Voice Match. https://support.google.com/assistant/answer/9071681?co=GENIE.Platform%3DAndroid&hl=en-GB

[54] Stefan Gössling, Mia Larson, and Aurimas Pumputis. 2021. Mutual surveillance on Airbnb. *Annals of Tourism Research* 91 (2021), 103314.

[55] Thomas Gross. 2021. Validity and Reliability of the Scale Internet Users' Information Privacy Concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies* 2021 (2021), 235 – 258.

[56] Hana Habib and Lorrie Faith Cranor. 2022. Evaluating the usability of privacy choice mechanisms. In *18th Symposium on Usable Privacy and Security*. 273–289.

[57] Rakibul Hasan, Rebecca Weil, Rudolf Siegel, and Katharina Krombholz. 2023. A Psychometric Scale to Measure Individuals' Value of Other People's Privacy (VOPP). In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–14.

[58] Weijia He, Nathan Reitinger, Atheer Almogbil, Yi-Shyuan Chiang, Timothy J Pierson, and David Kotz. 2024. Contextualizing Interpersonal Data Sharing in Smart Homes. *Proceedings on Privacy Enhancing Technologies* (2024).

[59] Weijia He, Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, Earlence Fernandes, Josiah Hester, and Blase Ur. 2021. SoK: Context Sensing for Access Control in the Adversarial Home IoT. In *IEEE European Symposium on Security and Privacy*. 37–53.

[60] Natali Helberger and Joris van Hoboken. 2010. Little brother is tagging you–Legal and policy implications of amateur data controllers. *Computer law review international* 11, 4 (2010), 101–109.

[61] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*. 1–13.

[62] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A survey on interdependent privacy. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–40.

[63] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In *ACM Conference on Human Factors in Computing Systems*. 1–19.

[64] Mark Johnson, Maggy Lee, Michael W. Mccahill, and Marian Mesina. 2019. Beyond the 'All Seeing Eye': Filipino Migrant Domestic Workers' Contestation of Care and Control in Hong Kong. *Ethnos* 85 (2019), 276 – 292.

[65] Bei Ju, Xiao Yang, X. H. Pu, and T. L. Sandel. 2023. (Re)making live-in or live-out choice: the lived experience of Filipina migrant domestic workers in Macao. *Gender, Place & Culture* 0, 0 (2023), 1–22.

[66] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *ACM Conference on Human Factors in Computing Systems*. 14 pages.

[67] Martin J. Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring Communal Technology Use in the Home. In *ACM Halfway to the Future Symposium*. 8 pages.

[68] Martin J. Kraemer, Ulrik Lyngs, Helena Webb, and Ivan Flechais. 2020. Further Exploring Communal Technology Use in Smart Homes: Social Expectations. In *ACM Conference on Human Factors in Computing Systems: Extended Abstracts*. 1–7.

[69] Priya C Kumar, Michael Zimmer, and Jessica Vitak. 2024. A Roadmap for Applying the Contextual Integrity Framework in Qualitative Privacy Research. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–29.

[70] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2 (2018), 1–31.

[71] Hosub Lee and Alfred Kobsa. 2016. Understanding user privacy in Internet of Things environments. In *IEEE 3rd World Forum on Internet of Things*. 407–412.

[72] Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. In *ACM Conference on Designing Interactive Systems*. 527–539.

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

[74] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res.* 15 (2004), 336–355.

[75] Nathan Malkin. 2023. Contextual Integrity, Explained: A More Usable Privacy Definition. *IEEE Security & Privacy* 21, 1 (Jan. 2023), 58–65.

[76] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. "What *can't* data be used for?" Privacy expectations about smart TVs in the U.S.. In *European Workshop on Usable Security*.

[77] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 250–271.

[78] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 436–458.

[79] Karola Marky, Nina Gerber, Michelle Gabriela Pelzer, Mohamed Khamis, and Max Mühlhäuser. 2022. "You offer privacy like you offer tea": Investigating mechanisms for improving guest privacy in IoT-equipped households. *Proceedings on Privacy Enhancing Technologies* (2022).

[80] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia*. 83–95.

[81] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2021. Roles matter! Understanding differences in the privacy mental models of smart home visitors and residents. In *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia*. 108–122.

[82] Karola Marky, Alina Stöver, Sarah Prange, Kira Bleck, Paul Gerber, Verena Zimmermann, Florian Müller, Florian Alt, and Max Mühlhäuser. 2024. Decide Yourself or Delegate: User Preferences Regarding the Autonomy of Personal Privacy Assistants in Private IoT-Equipped Environments. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, 20 pages.

[83] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *ACM Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. 11 pages.

[84] Kirsten Martin and Helen Nissenbaum. 2016. Measuring privacy: an empirical test using context to expose confounding variables. *Columbia Science & Technology Law Review* 18 (2016).

[85] Frank J Massey Jr. 1951. The Kolmogorov-Smirnov test for goodness of fit. *Journal of the American statistical Association* 46, 253 (1951), 68–78.

[86] Nicole Meng, Dilara Kekülluoğlu, and Kami Vaniea. 2021. Owning and Sharing: Privacy Perceptions of Smart Speaker Users. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW (April 2021), 29 pages.

[87] Nicole Meng-Schneider, Rabia Yasa Kostas, Kami Vaniea, and Maria K Wolters. 2023. Multi-User Smart Speakers—A Narrative Review of Concerns and Problematic Interactions. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 7 pages.

[88] Alessandro Montanari, Afra Mashhadi, Akhil Mathur, and Fahim Kawsar. 2016. Understanding the Privacy Design Space for Personal Connected Objects. In *International BCS Human Computer Interaction Conference: Fusion*. BCS Learning & Development Ltd., 18:1–18:13.

[89] Pratik Musale and Adam Lee. 2023. Trust TEE?: Exploring the impact of trusted execution environments on smart home privacy norms. *Proceedings on Privacy Enhancing Technologies* 2023 (2023). Issue 3.

[90] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *The proceedings of 13th symposium on usable privacy and security)*. 399–412.

[91] John Neter, Michael H Kutner, Christopher J Nachtsheim, William Wasserman, et al. 1996. Applied linear statistical models. (1996).

[92] Helen Nissenbaum. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life.

[93] Helen Nissenbaum. 2014. Respect for context as a benchmark for privacy online: What it is and isn't. *Cahier de prospective* 19 (2014).

[94] Helen Nissenbaum. 2019. Contextual integrity up and down the data food chain. *Theoretical Inquiries in Law* 20, 1 (2019), 221–256.

[95] State of California. 2018. California Consumer Privacy Act (CCPA). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.

[96] Sunyup Park, Weijia He, Elmira Deldari, Pardis Emami-Naeini, Danny Yuxing Huang, Jessica Vitak, Yaxing Yao, and Michael Zimmer. 2024. Well-intended but half-hearted: Hosts' consideration of guests' privacy using smart devices on rental properties. In *The Proceedings of the 20th Symposium on Usable Privacy and Security*. USENIX Association, 179–198.

[97] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurle, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. 2022. Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras. In *ACM Conference on Designing Interactive Systems*.

[98] Nicholas Proferes. 2022. The Development of Privacy Norms. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing.

[99] Joel R Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T Graves, Fei Liu, Aleecia McDonald, Thomas B Norton, Rohan Ramanath, et al. 2015. Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Tech. LJ* 30 (2015), 39.

[100] Eimaan Saqib, Shijing He, Junghyun Choy, Ruba Abu-Salma, Jose Such, Julia Bernd, and Mobin Javed. 2025. Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions. *ACM Transactions on Computer–Human Interaction* (2025). To appear.

[101] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. 2017. Designing effective privacy notices and controls. *IEEE Internet Computing* 21, 3 (2017), 70–77.

[102] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Eleventh symposium on usable privacy and security (SOUPS 2015)*. 1–17.

[103] Roei Schuster, Vitaly Shmatikov, and Eran Tromer. 2018. Situational access control in the internet of things. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 1056–1073.

[104] Juliet Popper Shaffer. 1995. Multiple hypothesis testing. *Annual review of psychology* 46, 1 (1995), 561–584.

[105] Yan Shvartzshnaider, Schrasing Tong, Thomas Wies, Paula Kift, Helen Nissenbaum, Lakshminarayanan Subramanian, and Prateek Mittal. 2016. Learning privacy expectations by crowdsourcing contextual informational norms. In *Fourth AAAI conference on human computation and crowdsourcing*.

[106] Amit Kumar Sikder, Leonardo Babun, Z Berkay Celik, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A Selcuk Uluagac. 2022. Who's controlling my device? Multi-user multi-device-aware access control system for shared smart home environment. *ACM Transactions on Internet of Things* 3, 4 (2022), 1–39.

[107] Julia Słupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. 2022. "They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers. In *Proceedings of the USENIX Security Symposium*.

[108] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *ACM Conference on Human Factors in Computing Systems*. 1–13.

[109] Statista. 2023. Smart home device ownership in the U.S. as of June 2023. https://www.statista.com/forecasts/997160/smart-home-device-ownership-in-the-us. Last accessed 26-September-2023.

[110] Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. 2019. Protection, productivity and pleasure in the smart home: Emerging expectations and gendered insights from Australian early adopters. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.

[111] Jennifer Jiyoung Suh and Miriam J. Metzger. 2022. Privacy Beyond the Individual Level. In *Modern Socio-Technical Perspectives on Privacy*, Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano (Eds.). Springer International Publishing.

[112] Iraklis Symeonidis, Gergely Biczók, Fatemeh Shirazi, Cristina Pérez-Solà, Jessica Schroers, and Bart Preneel. 2018. Collateral damage of Facebook third-party applications: a comprehensive study. *Computers & Security* 77 (2018), 179–208.

[113] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. "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*. 435–450.

[114] Madiha Tabassum and Heather Lipford. 2023. Exploring privacy implications of awareness and control mechanisms in smart home devices. *Proceedings on Privacy Enhancing Technologies* 2023 (01 2023), 571–588.

[115] Neilly H. Tan, Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. 2022. Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In *ACM CHI Conference on Human Factors in Computing System*. 1–25.

[116] Jack E Taylor, Guillaume A Rousselet, Christoph Scheepers, and Sara C Sereno. 2023. Rating norms should be calculated from cumulative link mixed effects models. *Behavior research methods* 55, 5 (2023), 2175–2196.

[117] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It would probably turn into a social faux-pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In *ACM Conference on Human Factors in Computing Systems*. 1–13.

[118] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 129–139.

[119] Christine Utz, Steffen Becker, Theodor Schnitzler, Florian M. Farke, Franziska Herbert, Leonie Schaewitz, Martin Degeling, and Markus Dürmuth. 2021. Apps Against the Spread: Privacy Implications and User Acceptance of COVID-19-Related Smartphone Apps on Three Continents. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, 1–22.

[120] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 973–990.

[121] Brendan Van Alsenoy. 2016. *Regulating data protection: The allocation of responsibility and risk among actors involved in personal data processing*. Ph. D. Dissertation. KU Leuven.

[122] Kristina P Vatcheva, MinJae Lee, Joseph B McCormick, and Mohammad H Rahbar. 2016. Multicollinearity in regression analyses conducted in epidemiologic studies. *Epidemiology (Sunnyvale, Calif.)* 6, 2 (2016).

[123] Jessica Vitak, Priya C Kumar, Yuting Liao, and Michael Zimmer. 2023. Boundary regulation processes and privacy concerns with (non-) use of voice-based assistants. *Human-Machine Communication* 6, 1 (2023), 10.

[124] Jessica Vitak, Yuting Liao, Anouk Mols, Daniel Trottier, Michael Zimmer, Priya C. Kumar, and Jason Pridmore. 2022. When Do Data Collection and Use Become a Matter of Concern? A Cross-Cultural Comparison of U.S. and Dutch Privacy Attitudes. *International Journal of Communication* 17, 0 (Dec. 2022), 28.

[125] Zixin Wang, Danny Yuxing Huang, and Yaxing Yao. 2023. Exploring tenants' preferences of privacy negotiation in Airbnb. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security '23)*. 535–551.

[126] Miranda Wei, Pardis Emami Naeini, Franziska Roesner, and Tadayoshi Kohno. 2023. Skilled or Gullible: Gender Stereotypes Related to Computer Security and Privacy. *IEEE Symposium on Security and Privacy* (2023), 2050–2067.

[127] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proceedings of the ACM on Human-Computer Interaction* 6, MHCI (Sept. 2022), 184:1–184:21. https://doi.org/10.1145/3546719

[128] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proceedings of the Conference on Human Factors in Computing Systems*. ACM, 16 pages.

[129] Richmond Y. Wong, Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. Broadening Privacy and Surveillance: Eliciting Interconnected Values with a Scenarios Workbook on Smart Home Cameras. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*. Association for Computing Machinery, 1093–1113.

[130] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata McDonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[131] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *USENIX Symposium on Usable Privacy and Security*. 65–80.

[132] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *28th USENIX Security Symposium*. 159–176.

[133] Shikun Zhang, Yan Shvartzshnaider, Yuanyuan Feng, Helen Nissenbaum, and Norman Sadeh. 2022. Stop the Spread: A Contextual Integrity Perspective on the Appropriateness of COVID-19 Vaccination Certificates. In *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency*. 1657–1670.

[134] Yuhang Zhao, Yaxing Yao, Jiaru Fu, and Nihan Zhou. 2022. 'If sighted people know, I should be able to know:' Privacy Perceptions of Bystanders with Visual Impairments around Camera-based Technology. arXiv:2210.12232 [cs.HC]

[135] Haozhe Zhou, Mayank Goel, and Yuvraj Agarwal. 2024. Bring Privacy To The Table: Interactive Negotiation for Privacy Settings of Shared Sensing Devices. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, 1–22.

A Participant instructions

Below is the text of the instructions we showed to the participants after they clicked on the survey link in Prolific..

Welcome to the survey about smart homes. To make sure we're on the same page, let us clarify what we mean by that. A smart home refers to a home setup where appliances and devices can be automatically and remotely controlled using a mobile or other networked device, and interconnected through the internet connection.

In this survey we will ask you to imagine different situations involving smart home devices and ask your opinions about them. Most of those questions will be about your personal opinions, there are no right or wrong answers; we really just want to learn what you think. Although some of the information or scenarios in the survey will be hypothetical, please try to answer as close as you can to what your honest response in real life would have been.

After these instructions we obtained participants' consent and asked them to solve a recaptcha for data quality assurance. Then we showed the device description (see Appx. B) and vignettes, and asked about the acceptability of the data flows in the vignettes, as described in §3.1. Finally, we asked them the exit survey questions (see Appx. C).

B Device descriptions

Descriptions of the devices that we showed to the participants:

Smart cameras are one example of smart home devices. They are vision systems with built-in sensors to capture images and/or audio. Smart cameras can analyze certain types of information in the images (for example, detect movement or recognize the identity of a visitor by face), and make decisions (for example, sending notifications to the user or a security service, or storing a recording).

Examples of smart cameras include: Ring (Amazon), Nest (Google), Cync, Arlo, Wyze, etc.

Smart speakers (also called voice assistants) are one example of smart home devices. They are internet-enabled speakers that are controlled by spoken commands. Smart speakers can stream songs and other audio content, relay information, and communicate with other devices.

Examples of smart speakers include: Echo Alexa (Amazon), Home Assistant (Google), HomePod with built-in Siri (Apple), Bixby (Samsung), Cortana (Microsoft), etc..

Smart door locks are one example of smart home devices. They are locks that open for an authorized user without a physical key, for example using a keypad, or wireless signal. Smart locks are connected to the Internet and can be operated remotely and keep track of when people use the door. For the purposes of this survey, we focus on smart locks that are **not** integrated with a camera.

Examples of smart locks include: Yale, Schlage, Kwikset, August, etc.

C Exit survey instrument

Q [factor importance ranking] When you were deciding whether the data sharing was acceptable, how important or unimportant were the following factors *(presented in random order)*:

- What data is being shared
- With whom the data is shared
- For what purposes the data is shared
- Whether the device's presence is disclosed
- Whether the specifics of data collection, use, sharing, and storage are disclosed
- How long the data is stored
- Whose data is shared
- Whether the collected data contains information about children
- Who (or what) shares the data (e.g. device owner, device itself, company that made the device, etc.)
- Where the device is located (e.g. private vs. common areas)
- What device collected the data
- What is my relationship with the person whose data is shared
- Other factors—please specify (choose 'Very unimportant' if there are no other factors you want to mention)

(Response options: 5-point Likert scale from "Very unimportant" to "Very important".)

Q [acceptance of data senders] How acceptable would it be if the following entities shared the [BYSTANDER's ROLE] data *(presented in random order)*:

- The device itself
- The company that made the device
- [DEVICE OWNER's ROLE]
- [BYSTANDER's ROLE]
- Other entity—please specify (choose 'Completely unacceptable' if there are no other entities you want to mention)

(Response options: 5-point Likert scale from "Completely unacceptable" to "Completely acceptable".)

Q [acceptance of data retention policies] How acceptable would it be if [BYSTANDER's ROLE]'s data was:

- Not saved/stored at any point
- Deleted immediately after the purpose of use is achieved
- Deleted after 1 month
- Kept until [BYSTANDER's ROLE] requested to delete it
- Kept indefinitely

(Response options: 5-point Likert scale from "Completely unacceptable" to "Completely acceptable". *Retention policy options were presented in random order.*)

Q [smart device experiences] From the list below, please select if you have encountered any of these smart internet-connected devices *(presented in random order)* in your home, other people's homes, or at work, or if you haven't encountered that device. Choose ALL that apply.

- Smart cameras (security camera, doorbell camera, nanny cam, smart baby monitor)
- Smart speakers/audio system (e.g., Amazon Echo, Google Home, Sonos One, Apple HomePod)
- Smart locks
- Smart home appliances (for lighting, controlling temperature, cooking, cleaning, taking care of the lawn/garden/pool, etc.)
- Wellness trackers (e.g. fitness trackers, sleep monitoring device)
- Gaming console (e.g., PlayStation, Xbox, etc.)
- Smart security & safety systems (smart garage door, leak detector, security/alarm system, smart smoke/carbon monoxide detector)
- Smart-device hub/controller (e.g., SmartThings Home Hub, Wink)
- Audio-only smart systems (audio-only baby monitor, audio-only security monitoring system)
- Smart displays (Amazon Echo Show, Meta Portal)
- Smart entertainment devices (smart TV, smart children's toys, streaming device like Chromecast)
- Other (please specify)

Q [comfort interacting with smart devices] In general, how comfortable are you with interacting with smart internet-connected devices?
(Response options: 5-point Likert scale from "Very uncomfortable" to "Very comfortable".)

Q [tech experience] Do you have education or work experience in any of the technical fields (such as Computer Science, Software Engineering, App Development, etc.)?
(Response options: Yes, No.)

Q [desired controls] As a [BYSTANDER'S ROLE], what kind of privacy control would you like to have over a [DEVICE]? / As a [DEVICE OWNER'S ROLE], what kind of privacy control would you like your [BYSTANDER'S ROLE] to have over a [DEVICE]?
(Free-form response.)

Q [participants' own privacy attitudes; IUIPC scale [55, 74]; calculated as the mean values for each participant] Please, indicate how much you agree or disagree with the following statements:

(1) Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
(2) Consumer control of personal information lies at the heart of consumer privacy.
(3) I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
(4) Companies seeking information online should disclose the way the data are collected, processed, and used.
(5) A good consumer online privacy policy should have a clear and conspicuous disclosure.
(6) It is very important to me that I am aware and knowledgeable about how my personal information will be used.
(7) It usually bothers me when online companies ask me for personal information.
(8) When online companies ask me for personal information, I sometimes think twice before providing it.
(9) It bothers me to give personal information to so many online companies.
(10) I'm concerned that online companies are collecting too much personal information about me.

(Response options: 5-point Likert scale from"Strongly disagree" to "Strongly agree".)

Q [attitudes toward the privacy of others; VOPP scale [57]; calculated as the mean values for each participant] You will see several statements concerning other people's privacy. Privacy means not disclosing information without consent of the involved persons. Please indicate how strongly you disagree or agree with these statements. There is no right or wrong answer. Please answer as honestly and accurately as possible.

(1) I respect other people's privacy without exception.
(2) I value other people's privacy more than most other people do.
(3) It is important for me to protect other people's privacy even when it is difficult to do so.
(4) Other people's privacy is valuable to me.
(5) When posting a photo with my friends online, it is important to ask for their permission first.
(6) It is important to keep myself from looking at other people's screen notifications.
(7) It is okay to listen to conversations of strangers in public places. (r)
(8) It is important to protect other people's privacy even if I need to invest time and efforts to do it.
(9) It is important to protect other people's privacy even if it ruins the fun for me.
(10) It is okay to screenshot conversations from private chats and show them to others. (r)
(11) It is okay to share other's contact information (such as phone number, email) on request, even when I'm not obliged to. (r)
(12) When sharing pictures of tourist attractions, it is important to ensure that nobody can be clearly identified.
(13) It is important to ask for consent before recording someone speaking.

(Response options: 5-point Likert scale from"Strongly disagree" to "Strongly agree". *Scale items marked with (r) are reverse-coded.*)

Q [experience with prior privacy/security violations] Have you ever experienced an information privacy or security violation/incident?
(Response options: Yes, No.)

(If answered Yes in the previous question.)
Q [timing of violation] When did the most recent information privacy or security violation/incident happen?
(Response options: Less than a month ago, 1-6 months ago, 6-12 months ago, More than a year ago.)

Q [experiences in role/situation] Have you ever been in any of the following roles? Choose ALL that apply.

- Guest in a smart home you rented on a short-term rental platform (such as Airbnb, VRBO, etc.)
- Host of a smart home you rented out on a short-term rental platform (such as Airbnb, VRBO, etc.)
- Housemate in a shared rental smart home
- Domestic worker in a smart home
- Employer of a domestic worker in your smart home
- Overnight guest in a friend's smart home
- Host of a friend visiting your smart home overnight
- None of the above

Q [comments] Do you have any comments about the study? (Free-form response.)

Moreover, the following attention checks were randomly inserted in the survey:

Q [attention check question 1] When you answer this question, could you please select never as a response option? (Never, Rarely, Sometimes, Often, Always)

Q [attention check question 2] After reading the description of this question, please choose neutral as your answer? (Very unlikely, Unlikely, Neutral, Likely, Very likely)

D Participants

Table 2: Summary of participants' demographics, background, and experiences.

	N	%
Gender		
Men	373	49.0
Women	369	48.5
Non-binary	16	2.1
Prefer not to say	3	0.4
Race or ethnicity		
White	565	74.2
Black	63	8.3
Asian	52	6.8
Mixed	52	6.8
Other	29	3.8
Highest level of education completed		
No formal qualifications	3	0.4
Secondary education	16	2.1
High school diploma	169	22.2
Technical/community college	125	16.4
Undergraduate degree	316	41.5
Graduate degree	112	14.7
Doctorate degree	18	2.4
Don't know / N/A / Unavailable	2	0.3
Student status		
No	649	85.5
Yes	109	14.5
Employment		
Full-time	550	72.3
Part-time	194	25.6
Unemployed (and job seeking)	8	1.1
Not in paid work	3	0.4
Other	5	0.7
Real-life experience in the Situations		
Housemate in a shared rental smart home	64	8.4
Overnight guest in a friend's smart home	305	40.1
Hosting a friend overnight in a smart home	154	20.2
Guest in a short-term rental smart home	230	30.2
Host of a short-term rental smart home	22	2.9
Employer of domestic worker in smart home	25	3.3
Domestic worker in smart home	47	6.2
None of the above	322	42.3
Total number of participants	761	

E Results of qualitative analysis

Table 3: Codebook of open-ended responses about the desired privacy controls for bystanders' data.

Code	Description	Example quote
Privacy controls		
None	Do not provide bystanders with any controls.	*"Since it isn't my home, I'd be okay with not having any privacy controls over the smart lock. I'd be content to leave the matter to the owner."* - P67
Feedback	Provide bystanders with the device feedback that it's on or recording (e.g. via lights or sounds).	*"A light indicating when the device is listening and collecting data."* - P287
Disclosure	Provide transparency (e.g. via notice, disclosures, explanations) about data collection, sharing, use, storage, and retention.	*"Disclosure of the lock itself, what it does, what info it collects, etc should all be given to the guest."* - P13
Consent	Obtain bystanders' consent or permission for data collection, sharing, use, and storage prior to data collection/sharing.	*"If they captured and recorded me without consent I would find that creepy."* - P217
Opt-out	Avoid collecting data in the first place, or allow bystanders to opt out of tracking, turn off the device, mute, physically remove or cover it, or avoid setting up voice profiles for devices activated with voice commands to avoid recognizing and recording their voices.	*"The ability to toggle it off entirely throughout the home, with a single switch. That switch ought to be very obviously located."* - P214
Not Internet-connected	Do not connect the smart home device to the Internet (e.g. process data locally, do not send it off to the cloud).	*"Maybe disconnect from WiFi."* - P130
Analog only	Use an analog device that doesn't generate or collect data.	*"I would like a regular bolt lock and something I feel more in control of."* - P4
Avoid usage	Avoid using or interacting with the smart device.	*"If I knew such a device was in use, I would not rent there."* - P562; *"I'd like them to be able to choose not to use it."* - P66
Change behaviour	Modify behaviour when device is recording (e.g. avoid having sensitive conversations).	*"I just want to know it's there, so I can be aware of what I say or do around it."* - P270
Discussion	Discuss the potential privacy controls, or negotiate the appropriate configuration of the settings with the bystanders, in order to reach an agreement that both the device owners and bystanders are comfortable with.	*"I would like to have gone over everything before setting it up so we could agree on parameters. I think if we are housemates who are equal, we should both have a say."* - P611
View data	Let bystanders view what data about them is is collected, stored, and shared. One (but not only) way of realizing it is to provide dashboard for bystanders, guest mode, or let them request a copy and export the data for offline review.	*"I would like my worker to be able to review video and audio of themselves upon request."* - P483
Limit data	Let bystanders have control over what specific data is collected or shared.	*"Being able to choose what info gets shared and what doesn't get shared."* - P15
Limit storage	Let bystanders control for how long the data is stored, and after that time elapsed automatically delete.	*"There should be storage for 30 days and auto deleted."* - P101; *"They can listen but not record me."* - P434
User deleting	Allow bystanders to delete their data.	*"To be able to access the saved footage and delete if wanted."* - P512.
Limit access	Let bystanders control who has access, especially whether any third parties can have access to it.	*"Be able to choose or not to choose if whether third parties can get access to info."* - P42; *"Being able to choose who can access the data."* - P92
Limit purpose	Let bystanders control for what purposes their data is collected, used, or shared.	*"I would like to limit it to the safety of the people in house, and troubleshooting."* - P41
Limit when	Limit the time frame when the data is collected (e.g. during business hours, on weekends, etc.).	*"That it can be turned off when they're not working or are doing something private."* - P80

Continued on next page

Table3 – continued from previous page

Code	Description	Example quote
Limit location	Limit what spaces the devices are located in (e.g. only in common spaces, only in device owner's own room, not in private spaces like bathrooms and bedrooms, or not in any indoor locations altogether).	*"I wouldn't want it to be in any bedroom or bathroom."* - P133
Obfuscation	Modify the data, e.g. to blur faces, change voices.	*"Facial blurring and voice distorting."* - P514; *"Perhaps they could have an option for blurring their appearance in the footage aside from their name or data associated with the blurred appearance."* - P522
Security controls		
Encryption	Encrypt the data.	*"I would like to know ... is our data encrypted."* - P157
Passwords	Have a strong, unique password for the account.	*"Ensure all account and device passwords are strong and unique."* - P470
Security	General mentioning of the security controls without specifics of how data should be secured, protected or how anonymity should be preserved.	*"Being able to keep sensitive private information secured."* - P129
Other themes		
Exceptions for control	Desire to have/provide transparency, but not active control.	*"I would not give control over to the domestic worker. But I would explain thoroughly every detail of the security camera in the home so that they are aware of their presence and what information is collected and shared."* - P644; *"I think he should have access to the content, but he should not be able to alter or delete content."* - P499
Exceptions for purposes	Desire to provide/have transparency or controls, but not in case of very important purposes like safety, crime activities/investigations, or emergency.	*"Nearly full control, with the exception of any sort of safety issues, damage or crimes."* - P143
Exceptions for access	Desire to provide/have transparency or controls, but be able to have the final say or access as the owner.	*"I'd like to have control over who shares my data, how my data is shared, and what data is shared with anyone other than my direct employer. I'd like to have control if my employer wants to share my data with 3rd parties, for instance requiring my permission."* - P27
Exceptions for the owner	Desire to provide/have transparency or controls over bystanders' data, but not over device owner's data.	*"I would like them to have the option to delete their data automatically after 30 days, but I wouldn't want them to have access to my records or usage."* - P11
Equal control	Provide bystanders with the same controls as the primary users.	*"With Adrian as a housemate privacy control needs to be decided by everyone in the house and should be equally allocated."* - P2
Trust	Privacy controls depend on the level of trust between the bystander and device owner or other data recipients.	*"It really depends on how comfortable I was with the friend. I like like access to logs and see how they are shared."* - P313
Invalid	Responses that we think are generated using AI or copied from the Internet.	
Unclear	Unclear what controls are suggested. General mentioning of controls for bystanders' data, without specifics.	

End of Table

Table 4: Summary of code occurrence counts for the open-ended responses about desired controls for bystanders' data. Percentages are calculated using the total N for the relevant column (see bottom row). "Sig." indicates what pairs of parameters (denoted by ~) are significantly different based on the Bonferroni-adjusted p values from the Chi-square or Fisher's exact tests. Symbols: 🔓 = smart door lock, 👁 = smart camera, 🎤 = smart speaker; 🏠 = housemates, 🛏 = Airbnb, 🛠 = Domestic work, 👥 = Friends.

Code	Total	Bystand.	Owner	Sig.	Lock	Speaker	Camera	Sig.	House.	Friends	Airbnb	Work	Sig.
Disclosure	160 (21.14%)	94 (22.93%)	66 (18.80%)		34 (17.80%)	44 (15.38%)	82 (28.87%)	🎤 ~ 👁	38 (20.11%)	36 (18.95%)	50 (25.51%)	36 (19.57%)	
Opt-out	130 (17.17%)	85 (20.73%)	45 (12.89%)		14 (7.33%)	67 (23.51%)	49 (17.25%)	🔓 ~ 👁	35 (18.42%)	37 (19.68%)	38 (19.39%)	20 (10.87%)	
Unclear	113 (14.93%)	50 (12.25%)	63 (17.95%)		36 (18.85%)	44 (15.44%)	33 (11.62%)		29 (15.34%)	23 (12.23%)	28 (14.29%)	33 (17.84%)	
Limit data	100 (13.21%)	61 (14.95%)	39 (11.17%)		18 (9.57%)	61 (21.4%)	21 (7.39%)	👁 ~ 🎤 🔓 ~ 🎤	28 (14.81%)	21 (11.17%)	28 (14.29%)	23 (12.50%)	
Limit access	97 (12.81%)	60 (14.71%)	37 (10.60%)		35 (18.62%)	30 (10.53%)	32 (11.27%)		27 (14.29%)	22 (11.70%)	27 (13.78%)	21 (11.41%)	
None	68 (8.98%)	25 (6.13%)	43 (12.32%)	Yes	25 (13.3%)	21 (7.37%)	22 (7.75%)		13 (6.88%)	21 (11.17%)	16 (8.16%)	18 (9.78%)	
Limit storage	66 (8.72%)	38 (9.31%)	28 (8.02%)		17 (9.04%)	26 (9.12%)	23 (8.10%)		16 (8.47%)	19 (10.11%)	16 (8.16%)	15 (8.15%)	
Limit location	54 (7.13%)	33 (8.05%)	21 (6.02%)		4 (2.09%)	7 (2.46%)	43 (15.14%)	🔓 ~ 👁 🎤 ~ 👁	11 (5.79%)	13 (6.91%)	16 (8.16%)	14 (7.61%)	
View data	53 (7.00%)	23 (5.64%)	30 (8.60%)		15 (7.98%)	10 (3.51%)	28 (9.86%)		15 (7.94%)	13 (6.91%)	14 (7.14%)	11 (5.98%)	
User deleting	47 (6.21%)	20 (4.90%)	27 (7.74%)		11 (5.85%)	15 (5.26%)	21 (7.39%)		8 (4.23%)	15 (7.98%)	13 (6.63%)	11 (5.98%)	
Exceptions	47 (6.21%)	11 (2.70%)	36 (10.32%)	Yes	17 (9.04%)	15 (5.26%)	15 (5.28%)		9 (4.76%)	16 (8.51%)	10 (5.10%)	12 (6.52%)	
Consent	43 (5.68%)	24 (5.88%)	19 (5.44%)		5 (2.66%)	13 (4.56%)	25 (8.80%)		14 (7.41%)	7 (3.72%)	11 (5.61%)	11 (5.98%)	🏠 ~ 👥 🛠 ~ 👥 🛏 ~ 👥
Equal control	29 (3.83%)	6 (1.47%)	23 (6.59%)	Yes	6 (3.19%)	8 (2.81%)	15 (5.28%)		7 (3.70%)	5 (2.66%)	6 (3.06%)	11 (5.98%)	
Limit purpose	26 (3.43%)	13 (3.19%)	13 (3.72%)		4 (2.13%)	9 (3.16%)	13 (4.58%)		7 (3.70%)	3 (1.60%)	8 (4.08%)	8 (4.35%)	
Purpose exceptions	25 (3.30%)	7 (1.72%)	18 (5.16%)		3 (1.60%)	12 (4.21%)	10 (3.52%)		3 (1.59%)	7 (3.72%)	9 (4.59%)	6 (3.26%)	
Avoid usage	24 (3.17%)	16 (3.92%)	8 (2.29%)		2 (1.06%)	10 (3.51%)	12 (4.23%)		6 (3.17%)	8 (4.26%)	4 (2.04%)	6 (3.26%)	
Limit when	13 (1.72%)	8 (1.96%)	5 (1.43%)		2 (1.06%)	6 (2.11%)	5 (1.76%)		3 (1.59%)	3 (1.60%)	5 (2.55%)	2 (1.09%)	
Trust	10 (1.32%)	6 (1.47%)	4 (1.15%)		0 (0.00%)	6 (2.11%)	4 (1.41%)		2 (1.06%)	2 (1.06%)	4 (2.04%)	2 (1.09%)	
Access exceptions	10 (1.32%)	4 (0.98%)	6 (1.72%)		7 (3.72%)	2 (0.70%)	1 (0.35%)	👁 ~ 🔓	4 (2.12%)	1 (0.53%)	1 (0.51%)	4 (2.17%)	
Obfuscation	9 (1.19%)	8 (1.96%)	1 (0.29%)		0 (0.00%)	3 (1.05%)	6 (2.11%)		2 (1.06%)	3 (1.60%)	2 (1.02%)	2 (1.09%)	
Security	9 (1.19%)	7 (1.72%)	2 (0.57%)		5 (2.66%)	2 (0.70%)	2 (0.70%)		2 (1.06%)	4 (2.13%)	0 (0.00%)	3 (1.63%)	
Discussion	9 (1.19%)	2 (0.49%)	7 (2.01%)		2 (1.06%)	2 (0.70%)	5 (1.76%)		3 (1.59%)	1 (0.53%)	0 (0.00%)	5 (2.72%)	
Control exceptions	8 (1.06%)	0 (0.00%)	8 (2.29%)		3 (1.60%)	1 (0.35%)	4 (1.41%)		2 (1.06%)	6 (3.19%)	0 (0.00%)	1 (0.54%)	
Feedback	6 (0.79%)	6 (1.47%)	0 (0.00%)		0 (0.00%)	5 (1.75%)	1 (0.35%)		0 (0.00%)	4 (2.13%)	1 (0.51%)	1 (0.54%)	
Analog only	6 (0.79%)	5 (1.23%)	1 (0.29%)		6 (3.19%)	0 (0.00%)	0 (0.00%)		0 (0.00%)	2 (1.06%)	3 (1.53%)	1 (0.54%)	
Change behavior	6 (0.79%)	4 (0.98%)	2 (0.57%)		0 (0.00%)	2 (0.70%)	4 (1.41%)		1 (0.53%)	1 (0.53%)	1 (0.51%)	3 (1.63%)	

Continued on next page

Table4 – continued from previous page

Code	Total	Bystand.	Owner	Sig.	Lock	Speaker	Camera	Sig.	House.	Friends	Airbnb	Work	Sig.
Invalid	6 (0.79%)	4 (0.98%)	2 (0.57%)		1 (0.53%)	4 (1.40%)	1 (0.35%)		2 (1.06%)	2 (1.06%)	1 (0.51%)	1 (0.54%)	
Not Internet-connected	5 (0.66%)	5 (1.23%)	0 (0.00%)		2 (1.06%)	1 (0.35%)	2 (0.70%)		0 (0.00%)	2 (1.06%)	1 (0.51%)	2 (1.09%)	
Owner exceptions	4 (0.53%)	0 (0.00%)	4 (1.15%)		4 (2.13%)	0 (0.00%)	0 (0.00%)		1 (0.53%)	2 (1.06%)	0 (0.00%)	1 (0.54%)	
Encryption	2 (0.26%)	2 (0.49%)	0 (0.00%)		1 (0.53%)	1 (0.35%)	0 (0.00%)		0 (0.00%)	1 (0.53%)	0 (0.00%)	1 (0.54%)	
Passwords	2 (0.26%)	1 (0.25%)	1 (0.29%)		0 (0.00%)	1 (0.35%)	1 (0.35%)		1 (0.53%)	0 (0.00%)	0 (0.00%)	1 (0.54%)	
Total responses	761	410	351		191	286	284		190	190	196	185	

End of Table

F Results of quantitative analyses

Table 5: Self-reported perceived importance of factors in determining acceptability of data practices.[a]

Factor	Very Important	Somewhat Important	Neutral	Somewhat Unimportant	Very Unimportant
With whom the data is shared	574 (75.4%)	141 (18.5%)	23 (3.0%)	13 (1.7%)	10 (1.3%)
For what purposes the data is shared	549 (72.1%)	159 (20.8%)	31 (4.0%)	11 (1.5%)	11 (1.5%)
What data is being shared	500 (65.7%)	191 (25.1%)	35 (4.6%)	18 (2.4%)	17 (2.2%)
Whose data is shared	431 (56.6%)	219 (28.8%)	61 (8.0%)	28 (3.7%)	22 (2.9%)
Who (or what) shares the data (e.g. device owner, device itself, company that made the device, etc.)	383 (50.3%)	255 (33.5%)	61 (8.0%)	35 (4.6%)	27 (3.6%)
Whether the device's presence is disclosed	348 (45.7%)	215 (28.3%)	109 (14.3%)	41 (5.4%)	48 (6.3%)
Whether the specifics of data collection, use, sharing, and storage are disclosed	337 (44.3%)	253 (33.3%)	102 (13.4%)	43 (5.7%)	26 (3.4%)
What is my relationship with the person whose data is shared/the person who shared the data	300 (39.4%)	251 (33.0%)	86 (11.3%)	73 (9.6%)	51 (6.7%)
Where the device is located (e.g. private vs. common areas)	205 (26.9%)	210 (27.6%)	148 (19.5%)	112 (14.7%)	86 (11.3%)
Whether the collected data contains information about children	248 (32.6%)	157 (20.6%)	185 (24.3%)	87 (11.4%)	84 (11.0%)
How long the data is stored	187 (24.6%)	180 (23.7%)	154 (20.2%)	136 (17.9%)	104 (13.7%)

[a] As the question asked "When you were deciding whether the data sharing was acceptable," participants who interpreted this literally may have marked "Neutral" or "Unimportant" for sender, data about children, and storage because they weren't mentioned in the vignettes. Results for those items may therefore be less reliable—however, as we noted in §3.1, sender may be strongly implied by recipient, making it a more active consideration.

Table 6: Ordinal regression analysis. Significance levels are marked by asterisks for Bonferroni-adjusted p values. Odds ratios (OR) represent a measure of the change in the acceptance level occurring for a one-unit increase in the predictor variable, holding all other variables constant.

	Independent Variables	**Dependent variable: Acceptance level**					
		Model 1			Model 2		
		β	OR	p	β	OR	p
Contextual	**Role (base: Device owner)**						
	Bystander	-0.251	0.778		-0.215	0.807	
	Device Type (base: Smart home camera)						
	Smart speaker	-0.568	0.567	***	-0.482	0.618	***
	Smart door lock	0.561	1.752	***	0.490	1.632	
	Data Format (base: Audio)						
	Logs/history of interactions with the device	0.176	1.193	***	0.176	1.192	***
	Video	-0.002	0.998		-0.004	0.996	
	Recipient (base: Device owner)						
	Government entity	-0.892	0.410	***	-0.889	0.411	***
	Device manufacturer's employees	-0.889	0.411	***	-0.886	0.412	***
	Device owner's contacts	-1.704	0.182	***	-1.702	0.182	***
	3rd-party company's employees	-1.471	0.230	***	-1.471	0.230	***
	Purpose (base: To ensure safety in the home)						
	To enforce house rules	-1.140	0.320	***	-1.136	0.321	***
	To assist in investigating a crime	0.573	1.774	***	0.575	1.777	***
	To share a memory	-1.384	0.251	***	-1.382	0.251	***
	To troubleshoot/improve device	-0.688	0.502	***	-0.688	0.503	***
	To monitor work	-1.730	0.177	***	-1.731	0.177	***
	To customize services/product recs	-1.547	0.213	***	-1.546	0.213	***
	Transparency (base: Did not tell)						
	Told and explained details	0.213	1.237		0.336	1.399	
	Told but didn't explain details	0.182	1.199		0.259	1.296	
	Situation (base: Shared housing)						
	Airbnb rental	-0.278	0.757		-0.286	0.751	
	Friend staying overnight	0.282	1.325		0.169	1.184	
	Domestic work	0.471	1.602		0.359	1.432	
Control	**Gender (base: Male)**						
	Female				0.241	1.273	
	Non-binary				-0.767	0.464	
	Education (base: Undergrad e.g. BA/BSc)						
	High school diploma/A-levels				0.562	1.754	***
	Secondary education (e.g. GED/GCSE)				0.422	1.525	
	Technical/community college				0.014	1.014	
	Graduate degree (MA/MSc/MPhil/other)				-0.379	0.685	
	Doctorate degree				0.592	1.808	
	Experience in a technical field (base: No)						
	Yes				0.116	1.123	
	Experience of privacy violation (base: No)						
	Yes				-0.101	0.904	
	Age				0.015	1.015	
	Comfort with IoT				0.370	1.448	***
	Concerns about privacy of others				0.005	1.005	
	IUIPC-Control				-0.043	0.958	
	IUIPC-Awareness				0.006	1.006	
	IUIPC-Collection				-0.084	0.919	***

End of table

Table 7: Ordinal regression analysis with interaction effects. Significance levels are marked by asterisks for Bonferroni-adjusted *p* values. Odds ratios (OR) represent a measure of the change in the acceptance level occurring for a one-unit increase in the predictor variable, holding all other variables constant.

	Independent Variables	**Dependent variable: Acceptance level**								
		Model 3			Model 4			Model 5		
		β	OR	p	β	OR	p	β	OR	p
Contextual	**Role (base: Device owner)**									
	Bystander	-0.255	0.775		-0.254	0.776		-0.256	0.774	
	Device Type (base: Smart home camera)									
	Smart speaker	-0.575	0.563	***	-0.574	0.563	***	-0.572	0.564	***
	Smart door lock	0.565	1.760		0.569	1.767		0.566	1.760	
	Data Format (base: Audio)									
	Logs/history of interactions with the device	0.178	1.195	***	0.178	1.195	***	0.178	1.195	***
	Video	-0.003	0.997		-0.002	0.998		0.000	1.000	
	Recipient (base: Device owner)									
	Government entity	-1.231	0.292	***	-0.763	0.466	***	-0.898	0.407	***
	Device manufacturer's employees	-1.297	0.273	***	-0.692	0.501	***	-0.896	0.408	***
	Device owner's contacts	-1.752	0.173	***	-1.493	0.225	***	-1.719	0.179	***
	3rd-party company's employees	-1.689	0.185	***	-1.317	0.268	***	-1.481	0.227	***
	Purpose (base: To ensure safety in the home)									
	To enforce house rules	-1.285	0.277	***	-1.139	0.320	***	-1.393	0.248	***
	To assist in investigating a crime	0.266	1.305	***	0.577	1.781	***	0.376	1.456	***
	To share a memory	-1.844	0.158	***	-1.387	0.250	***	-1.214	0.297	***
	To troubleshoot/improve device	-1.046	0.351	***	-0.683	0.505	***	-0.714	0.490	***
	To monitor work	-0.976	0.377	***	-1.726	0.178	***	-1.693	0.184	***
	To customize services/product recs	-1.586	0.205	***	-1.548	0.213	***	-1.537	0.215	***
	Transparency (base: Did not tell)									
	Told and explained details	0.213	1.237		0.222	1.248		0.218	1.244	
	Told but didn't explain details	0.182	1.199		0.193	1.213		0.190	1.209	
	Situation (base: Shared housing)									
	Airbnb rental	-0.278	0.757		-0.452	0.636		-0.377	0.686	
	Friend staying overnight	0.284	1.328		0.484	1.623		0.218	1.244	
	Domestic work	0.475	1.608		0.976	2.655	***	0.358	1.431	
Interactions	**Recipient × Purpose**									
	(base: Device Owner × To ensure safety in the home)									
	Device owner's contacts × To enforce house rules	-0.099	0.905							
	Government entity × To investigate a crime	0.797	2.218	***						
	Device manufacturer employees × To investigate a crime	0.256	1.292							
	Device owner's contacts × To investigate a crime	0.202	1.224							
	3rd-party company employees × To investigate a crime	0.307	1.359							
	Device owner's contacts × To share a memory	-0.591	0.554	***						
	Device manufacturer employees × To troubleshoot/improve	1.002	2.724	***						
	Device owner's contacts × To troubleshoot/improve	-0.236	0.790							
	Third-party company × To troubleshoot/improve	0.444	1.559	***						
	Government entity × To monitor work	-1.643	0.193	***						
	Device owner's contacts × To monitor work	-0.885	0.413	***						
	3rd-party company employees × To monitor work	-0.896	0.408	***						
	Device manufacturer employees × To customize services/recs	0.263	1.301							

Continued on next page

Table 7 – *continued from previous page*

Independent Variables	**Dependent variable: Acceptance level**								
	Model 3			Model 4			Model 5		
	β	OR	p	β	OR	p	β	OR	p
Recipient × Situation									
(base: Device Owner × Shared housing)									
Government entity × Airbnb rental				0.650	1.916	***			
Device manufacturer employees × Airbnb rental				0.329	1.389	***			
Device owner's contacts × Airbnb rental				-0.096	0.908				
3rd-party company employees × Airbnb rental				0.302	1.352	***			
Government entity × Friend staying overnight				-0.241	0.786				
Device manufacturer employees × Friend staying overnight				-0.440	0.644	***			
Device owner's contacts × Friend staying overnight				-0.053	0.948				
3rd-party company employees × Friend staying overnight				-0.334	0.716	***			
Government entity × Domestic work				-0.787	0.455	***			
Device manufacturer employees × Domestic work				-0.666	0.514	***			
Device owner's contacts × Domestic work				-0.696	0.499	***			
3rd-party company employees × Domestic work				-0.578	0.561	***			
Situation × Purpose									
(base: Shared housing × To ensure safety in the home)									
Airbnb rental × To enforce house rules							0.318	1.374	
Friend staying overnight × To enforce house rules							0.274	1.315	
Domestic work × To enforce house rules							0.407	1.503	***
Airbnb rental × To investigate a crime							0.336	1.399	***
Friend staying overnight × To investigate a crime							0.181	1.198	
Domestic work × To investigate a crime							0.291	1.338	***
Airbnb rental × To share a memory							-1.150	0.317	***
Friend staying overnight × To share a memory							0.368	1.445	
Domestic work × To share a memory							-0.115	0.891	
Airbnb rental × To troubleshoot/improve							0.136	1.145	
Friend staying overnight × To troubleshoot/improve							-0.072	0.930	
Domestic work × To troubleshoot/improve							0.035	1.035	
Airbnb rental × To customize services/recs							0.220	1.246	
Friend staying overnight × To customize services/recs							-0.225	0.798	
Domestic work × To customize services/recs							-0.033	0.968	

End of table

G Heatmaps

We present larger, more visible versions of the heatmaps from Figures 1, 2, and 3.

- Figure 1 illustrates the average acceptance scores for information flows across Data Format × Purpose of Sharing pairs. The heatmap for the Owner role is shown in Figure 4, while the heatmap for the Bystander role is in Figure 5.
- Figure 2 displays the average acceptance scores for information flows across Device × Purpose of Sharing pairs. The heatmap for the Owner role is provided in Figure 6, and the heatmap for the Bystander role appears in Figure 7.
- Figure 3 presents the average acceptance scores for information flows across Recipient × Purpose of Sharing pairs. The heatmap for the Owner role is shown in Figure 8, while the heatmap for the Bystander role is in Figure 9.

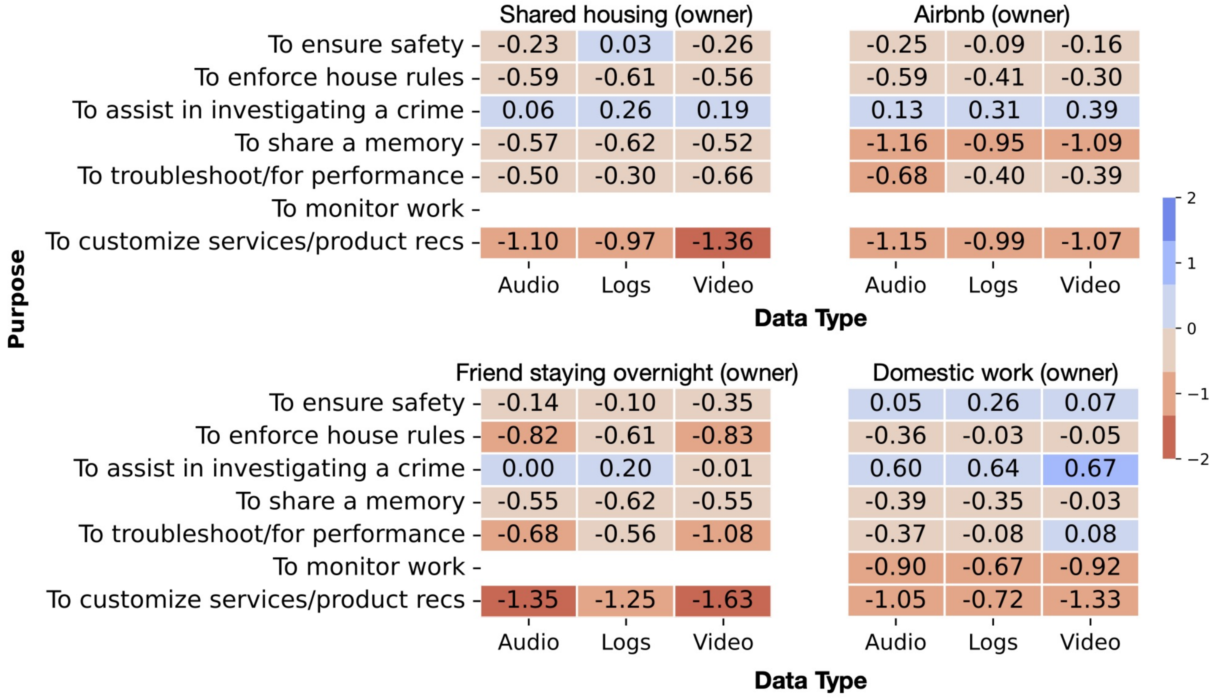

Figure 4: Average acceptance scores for information flows across Data formats × Purpose of sharing pairs – Owner Scenarios.

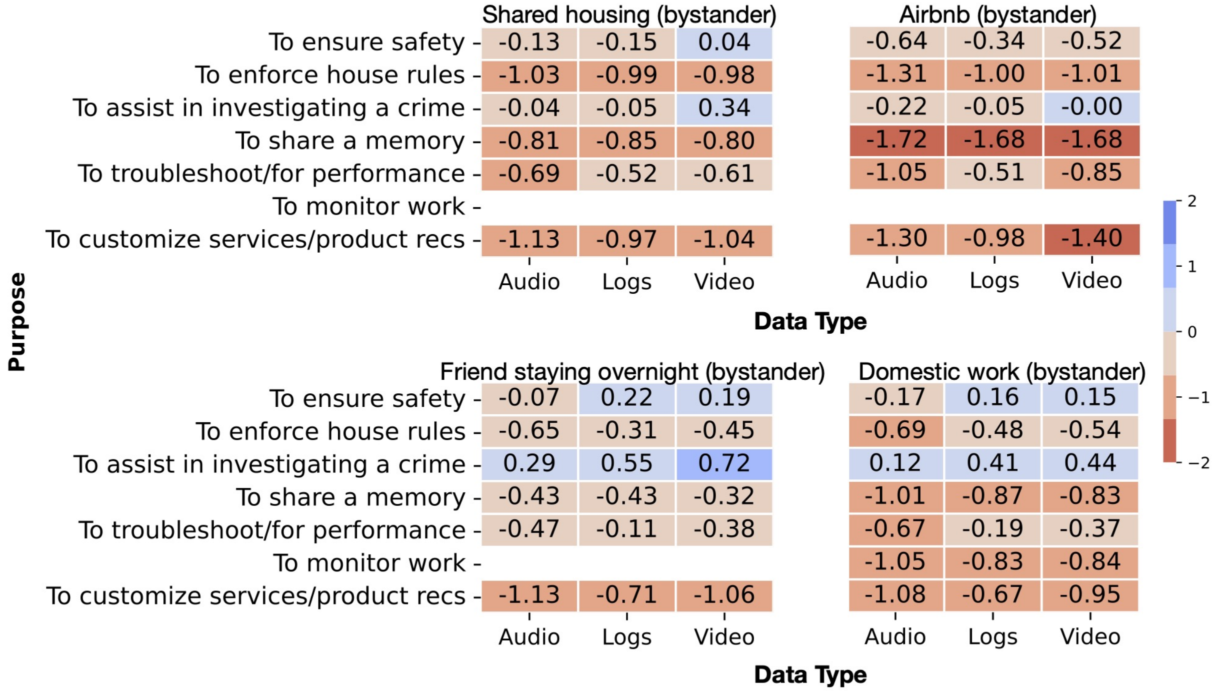

Figure 5: Average acceptance scores for information flows across Data formats × Purpose of sharing pairs – Bystander Scenarios.

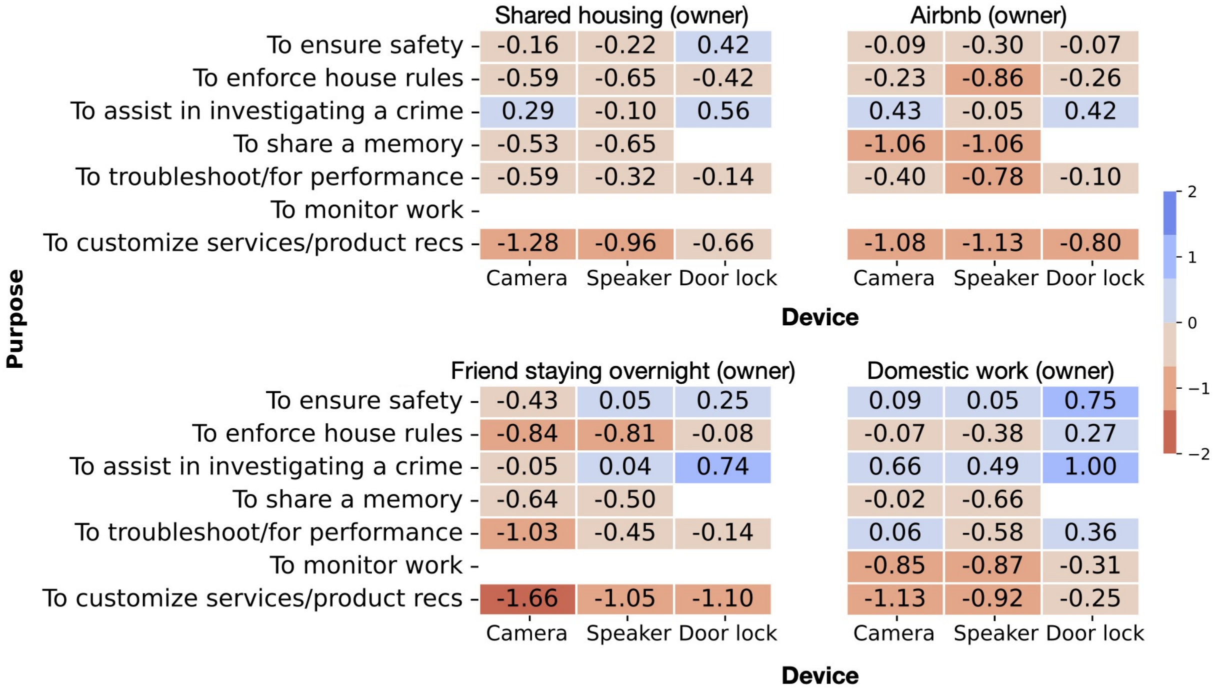

Figure 6: Average acceptance scores for information flows across Devices × Purpose of sharing pairs – Owner Scenarios.

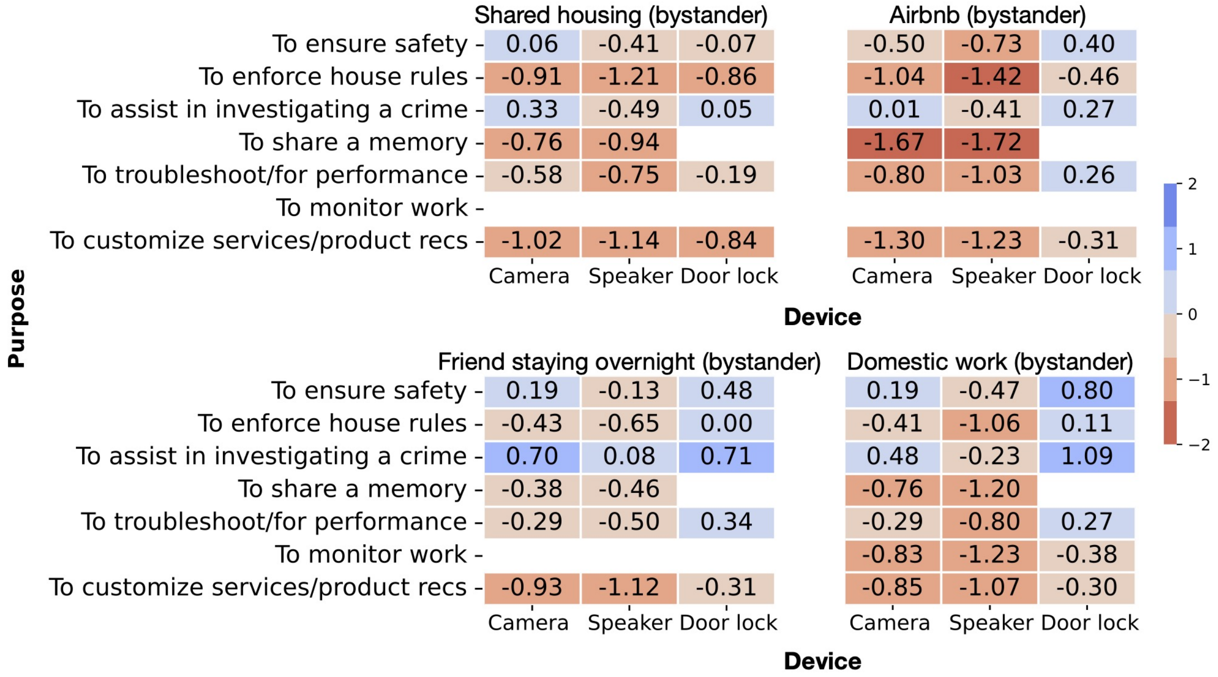

Figure 7: Average acceptance scores for information flows across Devices × Purpose of sharing pairs – Bystander Scenarios.

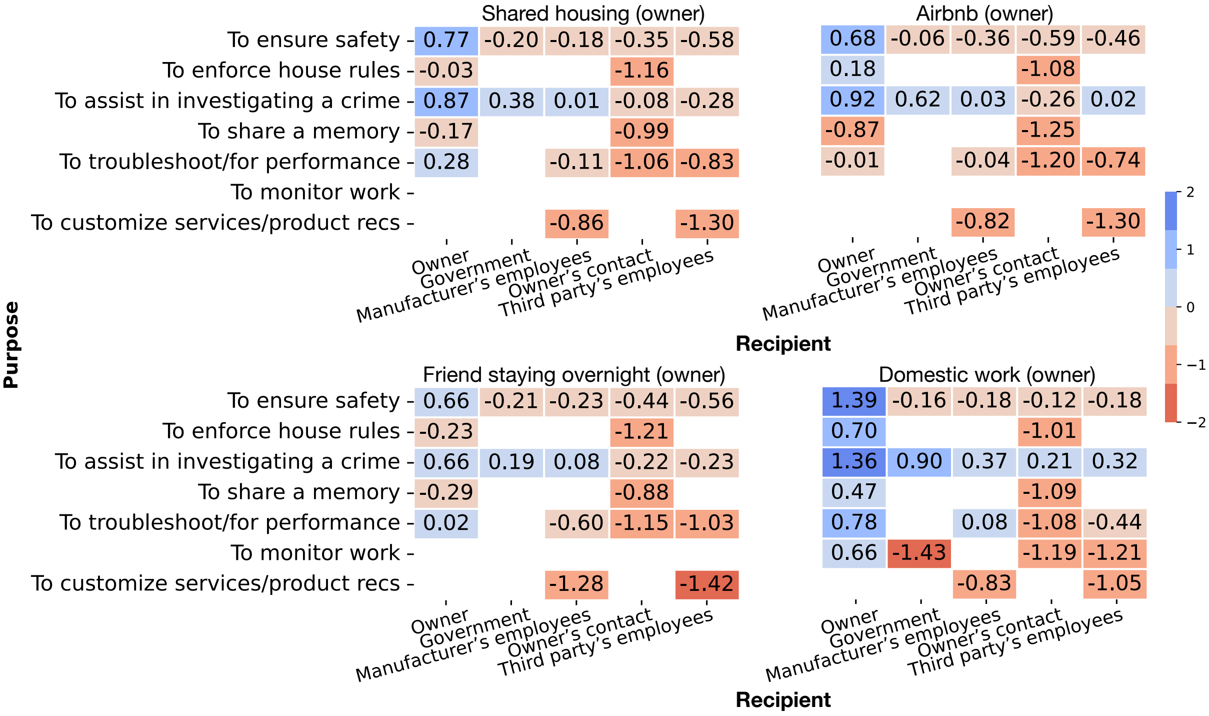

Figure 8: Average acceptance scores for information flows across Recipients × Purpose of sharing pairs – Owner Scenarios.

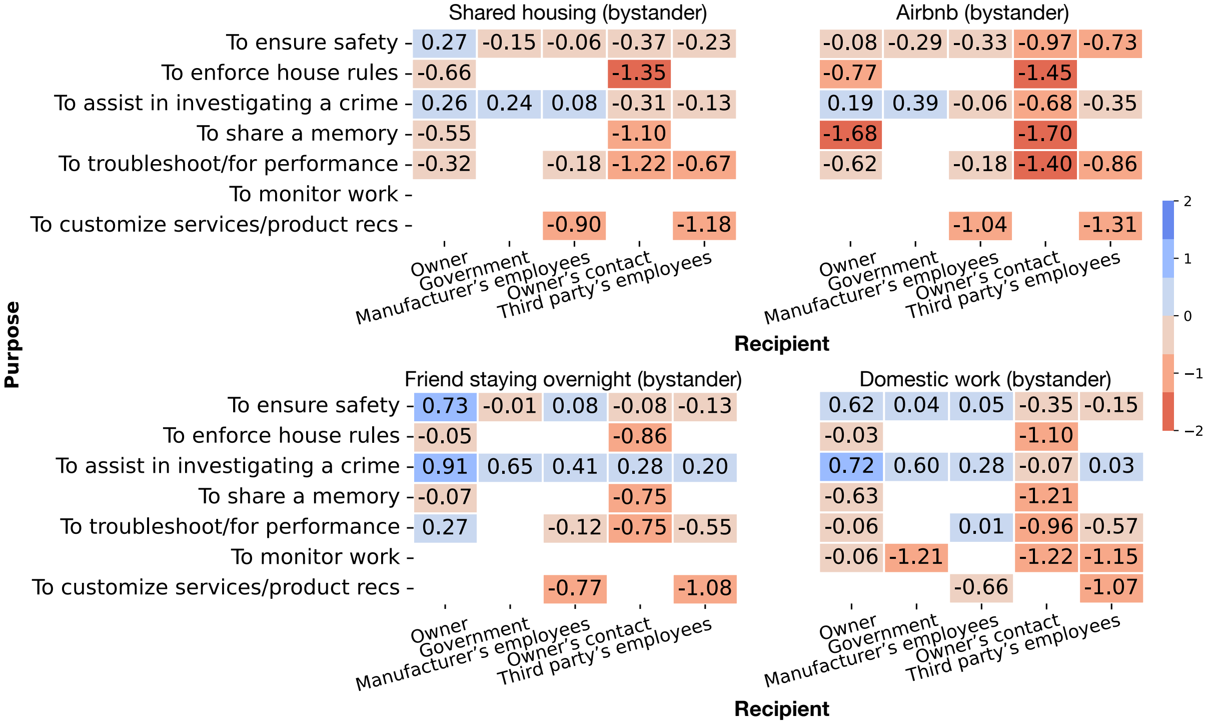

Figure 9: Average acceptance scores for information flows across Recipients × Purpose of sharing pairs – Bystander Scenarios.