More than just informed: The importance of consent facets in smart homes

Yi-Shyuan Chiang
yschiangg@gmail.com
University of Illinois Urbana-Champaign
Urbana, Illinois, United States

Omar Khan
omark807@gmail.com
University of Illinois Urbana-Champaign
Urbana, Illinois, United States

Adam Bates
batesa@illinois.edu
University of Illinois Urbana-Champaign
Urbana, Illinois, United States

Camille Cobb
camillec@illinois.edu
University of Illinois Urbana-Champaign
Urbana, Illinois, United States

ABSTRACT

Data collection without proper consent is a growing concern as smart home devices gain prevalence. It is especially difficult to obtain consent from incidental users because they may be unaware or feel pressured to consent. To understand what appropriate consent means in smart homes, we conducted an online survey (N=360) covering 6 common consent facets: *freely given*, *revertible*, *informed*, *enthusiastic*, *specific*, and *unburdensome*. We study how these facets affect perceived acceptability of data collection and how users would allocate responsibility for obtaining consent. Our results show that all facets have meaningful impacts on perceived acceptability of data collection, and eroding freely given had the greatest impact. Device owners were considered the most responsible for obtaining consent. Based on these findings, we provide recommendations for users, device manufacturers, and policymakers to improve consent practices in smart homes, such as designing consent interfaces that prioritize multiple facets of consent.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; • **Social and professional topics** → **Governmental regulations**; *Privacy policies*; • **Human-centered computing** → Empirical studies in HCI.

KEYWORDS

Consent, Incidental users, Smart home, Data collection

ACM Reference Format:
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 (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 21 pages. https://doi.org/10.1145/3613904.3642288

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642288

1 INTRODUCTION

As smart home devices become more common, it is vital to address their key privacy challenges. Smart home devices grant a sense of agency to users. For example, they can help enable seniors and people with disabilities to have control over their appliances [17, 18, 54]. However, they also present significant privacy risks. Numerous studies have identified security- and privacy-related risks that come with these devices, such as smart home devices being exploited for domestic violence [14, 32] or device manufacturers sharing video footage with police without permission [37]. Recent research has begun to acknowledge and address privacy risks that extend beyond those users who purchase and/or install smart home devices in their own homes [1, 2, 5, 11–13, 20, 50, 79, 82, 88].

We refer to these stakeholders as *incidental users* [20]; that is, people that come into contact with a device who are not the device's owner or controller. Unlike primary users who have access to smart systems, incidental users usually do not have the same amount of control. Domestic workers have reported discomfort toward being the surveillance targets of cameras, but as employees they might not be in a position to negotiate about device placement [11–13]. Similarly, house guests might not express their privacy concerns because of social pressures [88]. Other studies focused on similar or overlapping stakeholder groups use the terms *passenger users* [38] and *bystanders* [1, 5, 12, 13, 50, 82, 85, 88].

Studies have suggested that we need a better understanding of and approach to *consent* in the context of smart home data collection [55]. Legislation requires explicit *consent* to safeguard privacy rights. For example, Illinois state's Biometric Information Privacy Act (BIPA) requires written consent to gather biometric information [60]. European Union's (EU) General Data Protection Regulation (GDPR) lists consent as one of the legal bases to automate personal data processing [15, 62]. California Consumer Privacy Act (CCPA), an effort to inform consumers how businesses handle consumers' personal information, requires business to gather consent to sell minor consumers' personal information and grants rights for consumers to request deletion of their data [42]. However, incidental users often lack awareness of and control over the devices they encounter, and their data is collected without consent. Further, while the importance of being *informed* (e.g., about devices' behaviors) has emerged as a theme in prior work on incidental users [3, 55, 85, 88], other facets of consent have not been considered. Moreover, there is no substantial understanding regarding

who should be responsible for gathering consent in the smart home data collection context.

In this work, we seek to provide insights on the importance of different consent facets in smart device data collection scenarios. Drawing from existing multi-faceted consent frameworks for data collection [15, 34, 41, 70, 80, 89], we identify common assertions that consent should be *freely given*, *revertible*, *informed*, *enthusiastic*, *specific*, and *unburdensome* (Table 1). We also study which stakeholders are deemed responsible if consent is not obtained. Understanding these issues will allow us to prioritize which research, smart device development, and regulation efforts are most important going forward. Specifically, our work answers the following research questions:

- RQ1 To what extent does consent play a role in how people evaluate the acceptability of smart home devices that are collecting data about incidental users?
- RQ2 What consent facets have the most (or least) impact on how people assess the acceptability of smart home devices that are collecting data about incidental users?
- RQ3 Are there contexts where consent is more important?
- RQ4 To what extent do people think device owners, incidental users, and device manufacturers bear responsibility to gather consent?

To answer these questions, we conducted an online survey with 360 participants that represented a demographically representative sample of United States (US) adults. Participants rated the acceptability of smart home devices collecting data about incidental users in a variety of vignettes. (*This story is about Darla and Chuck...Chuck has a smart camera that records both video and audio on the bedside table.*) After obtaining a baseline acceptability rating for each vignette, we *eroded* one consent facet (*Darla was not enthusiastic about being around the smart camera.*), and then obtained a second, revised acceptability rating. After the vignette-based questions, participants directly rated the importance of consent facets, rated the responsibility level of smart home stakeholders, and answered questions about their own relevant experiences in smart homes. Our contributions include revealing the impact of consent (and eroding consent facets) on data collection acceptability, highlighting the equal importance of consent facets other than *informed* (e.g., *freely given)* in gathering consent, and proposing legal and design recommendations that future research directions can further explore to create more consentful smart homes. In doing so, we can begin to give incidental users the agency with respect to their data.

2 BACKGROUND AND RELATED WORK

Our study builds on existing research, academic literature, and relevant news articles from the following fields: smart home device development and benefits, security and privacy concerns in smart homes, experiences of incidental users in smart homes, and legal and social conceptions of consent.

2.1 Risks & benefits of owning smart home devices

Smart home devices such as smart speakers are now widely available and financially accessible to consumers throughout much of the world. As of 2022, 57.4 million US households actively use smart home devices [44]. Smart speakers, vacuum cleaners, doorbells, and security cameras are the most commonly installed devices in the US and Canada [68]. Smart speakers, smart displays, and smart thermostats are also common devices that have been rated as the best smart home devices to have in 2022 [56, 65]. Adopters use smart home devices for convenience, time-saving, enhanced home security, and enjoyment [67, 81]. Despite their potential benefits, smart home devices also raise important privacy concerns. Research has pointed out that smart home devices are prone to vulnerabilities such as software attacks, physical attacks, and encryption attacks [7]. Software attacks allow hackers to access sensitive information and disturb the system availability via smart home device adopters' home network [31]. With physical attacks, attackers are able to impose physical damages to the devices which directly affect the residents [43].

Zeng et al.'s study on smart home device threat models revealed that smart home device adopters were aware of the security and privacy issues [90]. Emami et al. also found that consumers took security and privacy into consideration when making smart home device purchases [24]. Huang et al. located adopters' privacy concerns such as data being sold to third parties, data used to determine behavioral patterns, or unauthorized access to personal information or misuse by unintended users in regards to housemates and external entities [33]. Reports have shown that smart home devices can be exploited by domestic abusers to affect household members by creating unpleasant home environments [14, 52]. To address smart home device adopters' concerns, researchers have proposed privacy labels that provide easy-to-understand insights on the privacy and security features [23].

2.2 Smart home device incidental users

Identifying incidental users Besides device adopters who own or set up the systems, smart home devices can be accessible to non-owners who share the same living environment. Earlier work identified device adopters' privacy concerns, and more recent work has moved beyond this, recognizing that non-adopters may also be affected by smart devices. Cobb et al. found several examples of jobs and professions that would involve people frequently being at houses that are not their own, such as nannies, delivery persons, caregivers, pest control professionals, and firefighters [20]. *Incidental users* and *bystanders* are two of the most common terms to define these non-adopters. Both describe people who are subject to smart home devices that they do not install, own, or have access to. *Incidental users* are "people who encounter smart home devices that are owned, controlled, and configured by someone else" [20]. *Bystanders* describes those who do not own or directly use the devices but are potentially involved in the use of smart home devices [88]. Researchers have also categorized the relationships based on whom introduce new smart home functionality (pilot-passenger) and the available interactions with smart home devices (primary user-secondary user-guest) [35, 38].

Privacy concerns and control mechanisms Scholars have studied privacy concerns of incidental users in various different contexts. A study on domestic workers in Jordan has discovered the complex interplay between religion, social norms, and privacy concerns [2].

Table 1: Consent facet details: which consent framework includes each facet and how the facet is conceptually described in relevant existing frameworks and legislation.

Consent facet	Relevant quotes from the reference frameworks
Freely given	**Affirmative consent** [25, 34]"An act that is forced (even if it results in pleasure and satisfaction despite the coercion) is non-consensual" ; "a person must not be pressured into agreeing to something against their will. They have to ... not be affected by other factors, such as being under the influence of alcohol or drugs to the point that they can't freely consent. If you're being pressured or manipulated to do something that you're not comfortable with, this may be a form of coercive control" **CCPA** [42] "'Consent' means any freely given, specific, informed, and unambiguous indication of the consumer's wishes" (1798.140.) **Consentful technology** [41] "... if an interface is designed to mislead people into doing something they normally wouldn't do, the application is not consentful." **GDPR** [61] "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 4 (11))
Revertible	**Affirmative consent** [34] "consent can be revoked at any time" **CCPA** [42] "A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer." (1798.105.) **Consentful technology** [41] "In technology, you should have the right to limit access or entirely remove your data at any time." **GDPR** [61] "The data subject shall have the right to withdraw his or her consent at any time." (Article 7 (3))
Informed	**Affirmative consent** [34] "People can only consent to an interaction after being given correct information about it — in an accessible way." **BIPA** "No private entity may ... obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject ... in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject ... in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used;" (740 ILCS 14/15) **CCPA** [42] See 1798.140. in *freely given*; "A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following..." (1798.100.) **Consentful technology** [41] "... use clear and accessible language to inform users about the risks they present and the data they are storing, rather than burying these important details in e.g., the fine print of terms and conditions." **GDPR** [61] See Article 4 (11) in *freely given*
Enthusiastic	**Affirmative consent** [34] "consent is not just the absence of coercion, but a strong desire to engage in the interaction" **Consentful technology** [41] "If people are giving up their data because they have to in order to access necessary services and not because they want to, that is not consentful."
Specific	**Affirmative consent** [34] "people should be able to consent to a particular action (or a particular person), and not a series of actions or people" **BIPA** See 740 ILCS 14/15 in *informed* **CCPA** [42] See 1798.140. in *freely given* **Consentful technology** [41] "... only uses data the user has directly given, not data acquired through other means like scraping or buying, and uses it only in ways the user has consented to." **GDPR** [61] See Article 4 (11) in *freely given*; "The request for consent shall be presented in a manner which is clearly distinguishable from the other matters."(Article 7 (2))
Unburdensome	**Affirmative consent** [34] "the costs associated with giving consent should not be so high that a person gives in and says 'yes' when they would rather say 'no"' **GDPR** [61] "... The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent." (Article 7 (3))

Others focused on understanding nannies' perceptions of camera data collection and the dynamics within the employing relationship [11–13]. Meng et al.'s study on intelligent personal assistants reported that incidental users bear similar concerns with device adopters, such as data collection and data selling [55]. Both Alshehri et al. and Windl et al.'s work have found that incidental users were concerned about the lack of control they have over their data [5, 85]. Cobb et al.'s study on the tension between incidental users and device owners had also shown incidental users had a general sense of unease, though they did not report specific privacy concerns [20]. Incidental users have various coping mechanisms to work around data collection, including but not limited to reducing the quality of data, blocking the stimulus, altering behaviors, and removing themselves from the data collection [1, 50, 85]. Researchers have also been working on privacy solutions for incidental users, for example, Yao et al. co-designed privacy tools with participants [87] and Thakkar et al. tested out various privacy awareness mechanisms for smart home devices [82].

2.3 Computers and consent

Data collection and "notice and consent" framework Current data collection policies mostly follow the "notice and consent" framework where people must be presented with related information before consenting [76]. Notifying allows people make informed decisions [73] so the framework has also been referred to as an "informed consent" framework [76]. Prior work found that some incidental users do subscribe to an informed consent mindset to manage privacy concerns [55] despite its limitations [45, 76]. People might suffer from consent fatigue [74], fail to grasp the importance of the data they give away [9], or have incorrect understandings of data collection mechanisms [26].

Ongoing efforts to improve technology-related consent procedures have made important progress in terms of regulating the way *first-hand* users give consent. For example, GDPR in the EU has resulted in more data collection consent dialogues on websites as consent has been one of the most common legal basis for data collection under Article 6 of GDPR [83]. The right to revoke consent has also been granted under GDPR Article (7)[63]. BIPA has required private entities who hold biometric information to meet requirements including notification obligation and getting written consent [22, 53]. Under CCPA business should inform consumers at or prior to the point of collection; consumers have the right to delete where they can request businesses to "delete any personal information about the consumer which the business has collected from the consumer" [59]. The right to delete can be delegated to authorized agents which means consumers don't have to mail in and keep track of every single one of the requests themselves [84]. For full text from data collection regulation please refer to Table 1.

Consent theory in human-computer interaction Besides regulation, more and more discussions about how human-computer interaction can benefit from different theories, such as affirmative consent theory and feminist lenses [34, 80], have also surfaced. Researchers have theorized a new conceptual framework from observing how consent has been implemented [58] The importance of communicating consent and device control from empirical studies has also been highlighted [40, 88, 91]. As the importance of communicating privacy is established, more focus has been on how to communicate privacy information properly, for example, Schaub et al. proposed guidelines for effective privacy notice design [72, 73]. Machuletz et al. compared different consent notices while Bermejo et al. focused on learning the behavioral difference when presented with various designs [10, 47]. The interview study conducted by Haney et al. revealed how participants assign privacy and security responsibilities [29]. In our study, we include frequently-mentioned consent facets from affirmative consent theory, consentful tech framework, BIPA, CCPA and GDPR: *freely given*, *revertible*, *informed*, *enthusiastic*, *specific*, and *unburdensome*. More specifically, we first referred to consentful tech framework [41] consist of *freely given*, *revertible*, *informed*, *enthusiastic*, and *specific*, cross-referenced facets from others sources, and added *unburdensome* from GDPR and Im et al. [34]. Please refer to Table 1 for consent facets, their sources, and how they are conceptually described.

3 METHODS

To understand the importance of consent for incidental users in smart homes, we conducted an online vignette-based survey. We used Prolific to recruit a participant sample demographically representative of US adults in terms of age, gender, and ethnicity (Table 2). There were no other inclusion or exclusion criteria. In total, we obtained 360 complete responses from 383 Prolific members who clicked through the invitation link. Average completion time was 14 minutes (median 12 minutes). We included two attention-check questions to ensure participants' response quality. We paid US$2.75 via Prolific after participants entered a completion code. The compensation is well above the US federal minimum wage and aligned with Prolific's suggested rates.

To reduce priming effects, we intentionally avoided using the word *consent* in the recruitment materials and earlier parts of the study. Our study was approved by our institutional review board, and we obtained informed consent from all participants (the word *consent did* appear in this part of the procedure). Recruitment materials and the full survey instrument can be found in Appendix A and B.

3.1 Survey procedure

The survey consisted of two main parts: vignette-based questions and direct questions regarding consent. In the vignette-based question section, participants read and reacted to three vignettes, short descriptions carefully constructed to vary characteristics that are relevant to the research questions [8, 27, 78]. In the direct questions about consent, participants indicated the extent to which they felt various consent facets were important and the extent to which they felt various parties (the device owner, the incidental user, and the device manufacturer) should be responsible for obtaining consent.

3.2 Vignette-based questions

This work is an exploratory study to understand the effect of consent facets, therefore, we focus on surveying a reasonable amount of combinations among common devices and scenarios from previous studies. Though it is not a full factorial design, this work

Table 2: Participant demographics, numbers in parentheses show the number of participants within that demographic.

Age	18-24 (50), 25-34 (61), 35-44 (60), 45-54 (62), 55 and above (126), Prefer not to say (1)
Gender	Female (179), Male (171), Non-binary (7), Prefer not to say (3)
Education	Less than a high school diploma, high school degree or equivalent, some college, no degree, or associate degree (154), Bachelor's degree (130), Master's degree (46), Professional degree (16), Doctorate (7), Prefer to self-describe (1), Prefer not to say (4)
Ethnicity	White or Caucasian (256), Black or African American (45), Asian or Pacific Islander (19), Hispanic or Latino (13), Native American or Alaskan Native (2), Mixed (21), Prefer not to say (4)

contributes an important initial understanding of how people think about multi-faceted consent in various smart home settings.

3.2.1 Vignette design and assignment. We built on prior work to design six vignettes that were realistic and for which we anticipated participants would have diverse baseline views on the acceptability of data collection. Past research has found that people's concern levels have correlated with device types and relationship types [30, 57]. For all vignettes, we varied two details: (1) Device type and (2) Relationship between device owners and incidental users. We included three Relationship types that were studied in prior work: employer-employee [2, 11–13], host-guest [49, 51], and co-residents [50]. Video and audio data (i.e., data collected by cameras) is especially sensitive [29, 57], so half of our vignettes include a camera as the Device type. In the remaining vignettes that featured Non-camera types, we prioritized the breadth of Device types: a smart speaker, smart door lock, and motion sensor.

Each vignette began by introducing the names of the incidental user and device owner and specifying their Relationship. We then described the context of exposure to the smart home device, such as how often or how long the incidental users were around the device. The vignettes ended with information about Device type, where it was located, and what data it collects. All vignettes are included in Table 3. To ensure participants saw diverse vignettes while avoiding survey fatigue, we applied the following criteria to generate six sets of three vignettes (see Table 3): (1) each set should contain (a) one of each Relationship type and (b) at most two about Smart Camera, and (2) each vignette should appear in exactly three sets. We randomly assigned one vignette set (Vignette set A, B, C, D, E, or F) to each participant and balanced across participants[1].

3.2.2 Baseline and revised acceptability ratings. For each vignette, participants provided two acceptability ratings: baseline ratings and revised ratings. The initial acceptability rating provided after participants read a vignette constituted a **baseline acceptability rating.** The second acceptability rating after participants read through consent erosion statements established a **revised acceptability rating**. The consent erosion statements depict how a specific consent facet was absent. Using our revised definitions, we created a set of statements that portrayed the lack of specific content facets without the explicit mention of the consent facets. The definitions and the corresponding erosion statements can both be found in Table 4. We randomly assigned the consent facet that was absent for each vignette. The consent facet eroded was randomized per vignette and balanced across all responses. That is, across all participants, each facet was eroded approximately the same number of times. We balanced the consent manipulation conditions such that each facet was eroded approximately the same number of times across all participants. Participants could explain their reasoning and, if their rating had changed, elaborate on why their ratings changed in free-response text fields. For example, this is what participants assigned to the Smart lock at rental vignette and the absence of *"informed"* would read through.

> [Randomly assigned vignette] This story is about Heather and Abigail. Heather is staying in Abigail's short-term rental cottage for a 7 day getaway vacation. Heather does not know Abigail personally. Abigail uses a smart lock that notifies and keeps a record of every time the door is locked or unlocked
>
> **Baseline acceptability rating** How do you feel about the smart lock [Device type] in this story collecting audio and video? (*Totally unacceptable* (1) to *Totally acceptable* (7))
>
> [Randomly assigned consent erosion statement] Suppose you found out that Abigail was not informed about the data collection of the smart lock.
>
> **Revised acceptability rating** How do you feel now? (*Totally unacceptable* (1) to *Totally acceptable* (7))

3.2.3 Direct questions about consent. After the vignette questions, we asked directly but broadly about consent to smart home devices' data collection. Participants read through a basic smart home scenario that involved an incidental user: *Jackie has a smart device made by IntelligentHome that collects data about Sam.* For each of the involved parties, i.e. device owners, incidental users, and manufacturers, participants then indicated the responsibility levels (*not responsible*, *somewhat responsible*, *a little responsible*, *very responsible*, and *don't know*) For example, participants were asked to what extent Jackie (the device owner) should be responsible for obtaining consent. Besides the three roles, participants could also list other parties that they find responsible by writing free responses and selecting their responsibility levels.

[1]Our vignette combination algorithm contains a mistake, therefore, Set A contained three camera types while Set F has no camera. Results from Kruskal-Wallis tests indicate there is no difference in terms of the distribution of acceptability ratings from Set A, Set F, and the rest of the sets that followed the original criteria ($p < 0.05$).

Table 3: We used the following six vignettes in our study. Vignettes feature a variety of relationship and device types. Each participant saw one of six sets of three vignettes.

Vignette	Relationship type	Device type	Vignette set membership
Delivery worker encounters smart doorbells: This story is about **Vincent** and Lewis. Vincent is a delivery driver. He has been delivering packages in the same residential areas for a little over a year, including Lewis's house. Vincent normally works 7-9 hours per day. He does not know anyone personally from the neighborhoods where he works. Many of the houses are equipped with smart doorbells that record video and audio.	Employer-employee	Smart camera	A, B, C
Plumber works near smart speaker: This story is about **Seth** and Pauline. Seth is a plumber. He has been hired to fix Pauline's dishwasher. Seth has been Pauline's go-to plumber in the past 10 years. Pauline has a smart speaker on the kitchen counter. The speaker has a microphone that records audio. Seth estimates the plumbing work at Pauline's house will only take an hour.	Employer-employee	Non-Smart camera: Smart speaker	D, E, F
Security camera captures neighbor's yard: This story is about **Mike** and Christina. Mike has been gardening for a couple of years now. Mike waters his front lawn every day and maintains the garden over the weekends. Christina is Mike's next-door neighbor. They exchange friendly waves and occasionally chat informally about house maintenance. Christina has installed a security camera that records video and audio. Even though the camera is pointed at her door, it also records video of Mike's yard and garden.	Co-residents	Smart camera	A, D, E
Motion sensor in newlyweds' home: This story is about **Geneva** and Nicolas. Geneva and Nicolas got married a year ago and moved into a new place together shortly after their wedding. Geneva works from home. Her home office is in the corner of the living room. Nicolas recently set up a motion sensor in the living room that records the presence of people.	Co-residents	Non-Smart camera: Motion sensor	B, C, F
Bedside camera in rental: This story is about **Darla** and Chuck. Darla is staying in Chuck's short-term rental apartment for one night. Darla does not know Chuck personally. Chuck has a smart camera that records both video and audio on the bedside table.	Host-guest	Smart camera	A, B, D
Smart lock at rental: This story is about **Heather** and Abigail. Heather is staying in Abigail's short-term rental cottage for a 7 day getaway vacation. Heather does not know Abigail personally. Abigail uses a smart lock that notifies and keeps a record of every time the door is locked or unlocked.	Host-guest	Non-Smart camera: Smart lock	C, E, F

Participants were then asked to consider a generic situation in which "person A" allows a smart home device to collect their data and rate their degree of agreement with ten consent-related statements on a 5-point Likert scale from *strongly disagree* (1) to strongly agree (5) [19, 75]. We randomized the order of the statements for each participant. These ten statements corresponded to the individual consent facets (Appendix 7). *Freely given*, *informed*, and *specific* have multiple statements as they can be interpreted differently [25, 46]. *Freely given* can be interpreted as being sober, not feeling pressured, and not being manipulated [25]. *Informed* also was further specified into three statements: being informed about the presence of device, how the device works, and what data the device collects. *Specific* can refer to: specify what is being allowed, and being sure whether they have allowed the data collection. For example, participants rated the extent to which they agreed with "It is important that person A is sober" (*freely given*).

3.3 Data analysis

3.3.1 Quantitative analysis. We conducted Wilcoxon signed-rank tests to compare whether this is differences between the baseline and revised acceptability ratings. Bayesian analysis is gaining increasing attention in the HCI community as it is able to report more precise effects and draw principled conclusions from smaller studies [36]. To test for the presence of these effects on sharing comfort levels, we perform linear regression modeling in the Bayesian framework with `Rstan` and `bayestestR` package in `R` [48, 66, 71]. In contrast to Null Hypothesis Significance Testing (NHST) in the

Table 4: Each time we showed participants a vignette, we eroded one of six consent facets. In the sentences used to erode consent in our survey, [incidental user] and [device] were filled in to match the vignette.

Consent facet	Erosion sentence
Freely-given	*[Incidental user] felt pressured into being around [device].*
Revertible	*[Incidental user] could not delete the data captured by [device].*
Informed	*[Incidental user] was not informed about the data collection by [device].*
Enthusiastic	*[Incidental user] was not enthusiastic about being around [device].*
Specific	*[Incidental user] could not specify details such as what would be recorded by [device].*
Undurdensome	It was very hard for *[incidental user] to stop the data collection of [device].*

Frequentist paradigm, which maps research into a binary question of whether to accept/reject the null hypothesis, Bayesian analysis directly estimates effect sizes. Further, it is not necessary to adjust for multiple comparisons when performing Bayesian analysis. An additional advantage of Bayesian analysis is the ability to quantify our existing beliefs of an effect, i.e., specifying a prior distribution. However, we have no basis for specifying a prior on our novel survey paradigm; therefore, we use an uninformative uniform prior distribution. This reflects, for example, a prior belief all devices in our vignettes will be associated with the same change scores. To confirm the conclusion drawn from the Bayesian accounts, we report the results of a frequentist linear regression model in Appendix D. The results from both accounts were the same in terms of whether study factors or consent facets have effects on changes in perceived acceptability ratings.

Our model uses rating changes, the difference between baseline and revised acceptability, as the outcome measure. Our predictor variables were: Device type (motion sensor, smart camera, smart lock, smart speaker), Relationship (employer-employee, co-residents, host-guest), and Consent facet (*freely given*, *revertible*, *informed*, *enthusiastic*, *specific*, and *unburdensome*). We used mean-centered effects coding to adjust for unequal amounts of observations between groups. For all predictors with more than two levels, we first compared the level associated with the highest change score (e.g., motion sensor) to the mean of the other levels (smart camera, smart lock, smart speaker). We then proceeded to perform nested comparisons where the level with the next highest change score is compared to the mean of the remaining levels. Finally, our model also includes a random intercept for participants to account for random variance in participant responses and participant-specific variances.

3.3.2 Qualitative analysis. There are three sets of free responses: explanations for acceptability rating changes (data set 1, 1080 responses), reasons for why certain parties are responsible for gathering consent (data set 2, 360 responses), and other parties that should be responsible for gathering consent (data set 3, 13 responses). The first and last authors familiarized themselves with all three data sets by reading all free-response data. The first author conducted open coding with 25% of data set 1 and 20% of data set 2. Because data set 3 contained so few responses, the conclusion we draw from data set 3 was derived from discussion between the first and last authors. Across multiple meetings, the first and last authors discussed open codes from both data sets 1 and 2. There were overlaps in the open codes that emerged from both data sets, therefore, we created one unified set of axial codes. The first and last authors then formalized the axial codes into a codebook.

The authors calculated the agreement coefficient between the coders with MAXQDA, a qualitative analysis software. To avoid paradoxical results in unequal marginal distributions, MAXQDA provides κ as the agreement coefficient. Proposed by Brennan and Prediger [16], κ can be interpreted with the benchmark notes for Cohen's Kappa [39]. For data sets 1 and 2, the first author explained the codebook to the second author, and they independently applied the codebook to all of data set 2. They started with data set 2 because it was smaller. After coding, the first and second authors discussed and manually resolved all disagreements. Resolving these disagreements helped the first author explain and correct misunderstandings of the codebook. For data set 1, they started by coding 5% of the data independently. κ was below an acceptable threshold, so they resolved all disagreements as before. We repeated this process with another 5% of data set 1 and this time reached a κ of 0.89, which is considered substantial reliability. We resolved disagreements manually. We considered this a signal that we could move forward with coding the data independently. Of the remaining 90% of data set 1, the first author coded 70%, and the second author coded 30%. The codebook can be found in Appendix E.

3.4 Limitations

The study is conducted with an all-U.S. participant pool. The results might not be generalized to other cultures and communities. We used survey platforms' logistics to balance the randomization over the entire participant pool; however, 9 participants saw the same consent facet erosion for all three vignettes. Repeated exposure might skew participants' acceptability ratings. Our work attempted to balance the breadth and width of vignettes, e.g. the scenarios and devices, in a scoped manner which resulted in this research covering only part of the combinations. We only specified relevant information to Device type and Relationship in our vignettes. Since other details relevant to scenarios and consent facets were unspecified, participants' default assumptions likely factored into their baseline acceptability ratings. For example, if a participant's default assumption was that it is normal to not be *informed* about the presence of a device, eroding this consent facet may not have affected their revised rating as much as it would have if not being *informed* were more unexpected. On the other hand, eroding other consent facets such as *freely given* may have subverted participants' expectations, leading to more significant shifts in their revised ratings. Some participants' explanations support this interpretation; for example, P227 did not change their rating after we eroded *specific* and explained: *"There is no change in the scenario largely because I assumed that to be the case."* We provided participants'

prior experiences of lack of consent facets to allow more contextual interpretation of the results. Besides the limitations stemming from the vignette designs, we unintentionally omitted a statement for *unburdensome*, so participants did not rate the importance of this facet. In 3.2.1 we described an algorithm to create sets of 3 vignettes; however, we located an error in our implementation of the algorithm which resulted in Set A including more 3 vignettes with cameras and Set F including no vignettes with camera. We run additional Krsukal-Wallis tests to confirm that the distributions of baseline acceptability, revised acceptability, and acceptability changes of Set A and Set F are not different from the rest of the vignette sets that do follow our original design.

4 RESULTS

In this section, we start by summarizing participants' prior real-world experiences with smart home devices and consent to provide context for their other responses. We then discuss how survey responses inform us about the importance of consent in smart homes broadly (RQ1) and about the relative importance of the consent facetes we manipulated (RQ2). Next, we examine how other factors such as device location and norms have intersectional influences on the importance of consent (RQ3). Finally, we describe how participants allocate responsibility in situations if consent is not obtained (RQ4).

4.1 Participants' experiences with smart home devices and consent

Participants had substantial prior experiences in the types of situations presented in our survey. 65% of participants (239) had installed, configured, or owned a smart home device. Of the device-owner participants, 76% of participants (181) stated that a domestic worker such as a babysitter, plumber, or delivery worker had worked in their homes.

88% of participants (317) had encountered smart home devices as incidental users, including as houseguests, neighbors, short-term housing renters, and/or domestic workers. 84% participants (304) had visited a house with smart home devices. Over half of participants' (201) neighbors had smart home devices outdoors, similar to our vignette *security camera captures neighbor's yard*. 86 participants – 46% of those who had stayed in short-term rentals such as VRBO or Airbnb in the past – reported seeing smart home devices there. This situation was represented by our *bedside camera in rental* and *smart lock at rental* vignettes. 50 participants – 50% of those who had worked as domestic workers such as babysitters, plumbers, or delivery workers – encountered smart home devices in this capacity. Our vignettes *delivery worker encounters smart doorbells* and *plumber works near smart speaker* captured this type of situation.

In keeping with our expectations based on prior work [20], which motivated our vignette design, participants most frequently encountered smart doorbells and security cameras when visiting others' house, in the neighborhood, or serving as domestic workers. When staying in short-term rentals, participants encountered smart doorbells the most.

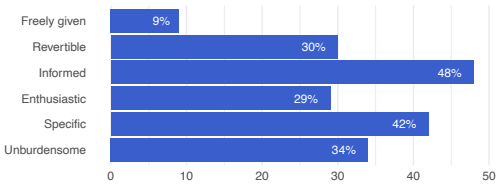

Figure 1: 84% of participants reported experiencing a situation in their own life in which a consent facet was absent. Most commonly, they were not *informed* about a device.

Selecting all that applied from a list of statements about personal experiences with consent in smart homes, the majority of participants (84%, 303 participants) reported encounters in which at least one consent facet was absent, as shown in Figure 1. Each statement was relevant to between 9% and 48% of participants. Most commonly, participants were not *informed*; 48% of participants (171) indicated that the following statement applied to them: *"I was not informed about the data collection process of someone else's smart home device(s)."* Participants selected the statement about *freely given* the least often, but still a significant portion of participants (9%, 33) indicated that *"I was pressured to be around someone else's smart home device(s) that were collecting data about me."*

4.2 RQ1: Consent has meaningful impact on acceptability of data collection

Our findings show that *yes,* consent (or lack thereof) *does* affect how people feel about the acceptability of smart home devices collecting data. First, the importance of consent emerged in participants' free-response answers; 10% of participants (37) explicitly mentioned *"consent"* or *"permission,"* even though we had not yet directly informed them that consent was a key focus of our study.

Second, considering all participants, all vignettes, and all consent manipulations, we examine participants' baseline and revised acceptability ratings (Figure 2). Out of 1080 baseline/revised acceptability ratings (three per participant), 58% (631) remained unchanged, 39% (421) decreased, and only 3% (28) increased after eroding consent. Although eroding consent did not always affect individual participants' acceptability judgments, mean acceptability dropped from 4.44 to 3.67 after erosion (mean change -0.76). The lower revised ratings indicate that participants tended to find data collection less acceptable when consent was eroded. This difference between the baseline and revised ratings is significant under a dependent measures Wilcoxon signed-rank test ($p < 0.05$).

4.3 RQ2: Some consent facets shape perceptions more

RQ2 addresses the role that specific consent facets – *freely given*, *revertible*, *informed*, *enthusiastic*, *specific*, and *unburdensome* – play in shaping how people think about the acceptability of smart home devices collecting data about incidental users. Using Wilcoxon signed-rank tests, we determined that the baseline and revised acceptability ratings were statistically different for all six consent facets ($p < 0.05$); that is, each individual consent facet was relevant to participants' overall assessments about the acceptability of data

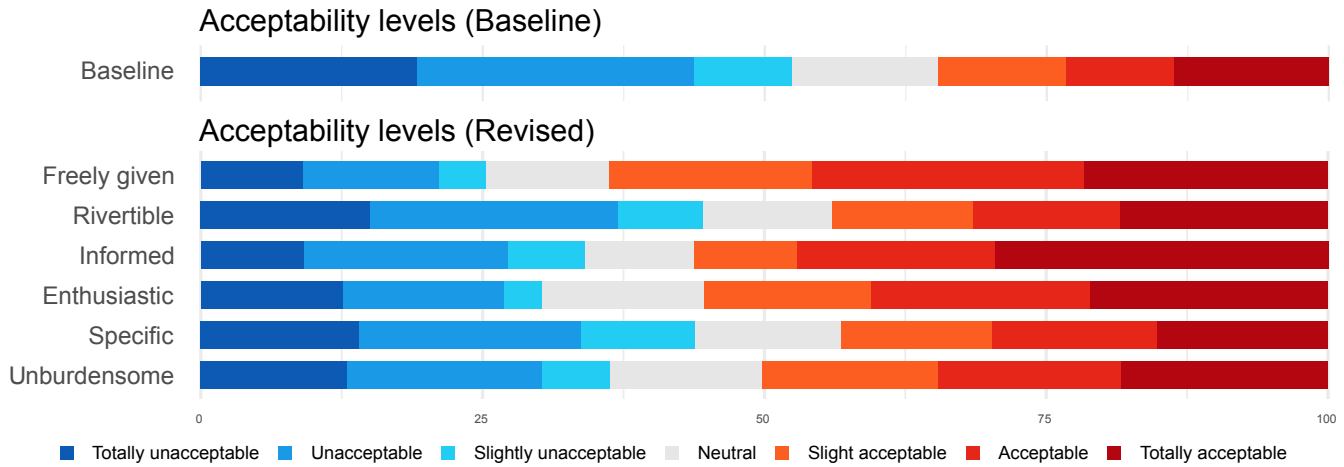

Figure 2: Participants rated the data collection in each vignette from totally acceptable (7) to totally unacceptable (1) both before we eroded a single consent facet (baseline) and after (revised). Revised acceptability scores tended to be lower across the board, but eroding *freely given* resulted in the largest deviation from the baseline while eroding *specific* had the least deviation.

Table 5: Summary of Bayesian linear mixed effects regression model. Estimates denote change in acceptability score. Credible Intervals denote 95% range of the posterior probability distributions for each comparison. Comparisons are *nested* such that each level in a variable is compared to the rows beneath it plus the reference level.

Variable	Estimate	Std. Dev.	Credible Interval
Intercept	-0.76	0.04	
Device type (Reference Level = Smart lock)			
Motion sensor	-0.36	0.14	[-0.64, -0.09]
Smart speaker	-0.16	0.12	[-0.39, 0.09]
Smart camera	-0.35	0.10	[-0.53, -0.14]
Relationship (Reference Level = Host-guest)			
Co-residents	-0.68	0.12	[-0.91, -0.47]
Employer-employee	-0.32	0.13	[-0.57, -0.07]
Consent facet (Reference Level = Specific)			
Freely given	-0.72	0.11	[-0.93, -0.51]
Informed	-0.35	0.11	[-0.55, -0.15]
Enthusiastic	-0.31	0.11	[-0.53, -0.11]
Unburdensome	-0.22	0.11	[-0.44, 0.00]
Revertible	-0.04	0.14	[-0.31, 0.23]

collection. However, some consent facets had a greater influence than others. Figure 2 shows that participants' acceptability ratings shifted most when we eroded *freely given* (-1.4) and least when we eroded *specific* (-0.4).

To better understand the relative contributions of the various trends identified throughout our results, we ran a linear mixed effects regression model in the Bayesian framework, the construction of which is described in Section 3.3. Our results are summarized in Table 5. Negative values for estimates and intervals indicate a *greater decrease* in acceptability. Compared to all other consent facets, *freely given* was associated with a -0.72 greater decrease in acceptability. To better evaluate the strength of this effect, we can refer to the 95% credible interval for this comparison – the lower bound on observed change is at least -0.51. Subsequent comparisons between different facets are nested, indicating that eroding *informed* decreases acceptability by -0.35 in comparison to all remaining facets. In these nested comparisons, the credible intervals for both *informed* and *enthusiastic* indicate a consistently observable effect on acceptability.

Besides inferring the acceptability from rating changes, we also asked participants to rate their agreement with the importance of individual consent facets. The trends from these direct ratings were somewhat well-aligned with participants' views inferred from their score changes (see Figure 3). More than half of the participants strongly or somewhat agreed that each consent facet was important. However, the relative importance placed on each facet did not align as well. For example, *informed* statements had the highest average agreement, but *informed* did not yield the highest inferred rating change. Likewise, even though *enthusiastic* had the most participants who somewhat or strongly disagreed with its importance, it was *specific* that had the lowest inferred rating change.

Many participants mentioned consent facets in their free response answers, suggesting that these facets held especially high salience or importance. *"Informed"* was the most-mentioned facet, which echos consent facet importance ratings. 30% of participants (106) wrote that the incidental user having knowledge of the device's presence (i.e., being informed or otherwise aware) was relevant to their thought process. For example, P110 wrote, *"If a person may be recorded, they should be informed prior to being recorded."* Going beyond mere awareness, 7% of participants (25) wrote that the data collection should be discussed with the incidental users instead of a one-way announcement. P325 wrote, *"I think Mike should be able to have a say in his yard being filmed and data of his property being collected."*

Supporting our other evidence about the importance of consent being *freely given*, 6% of participants (22) wrote that consent being

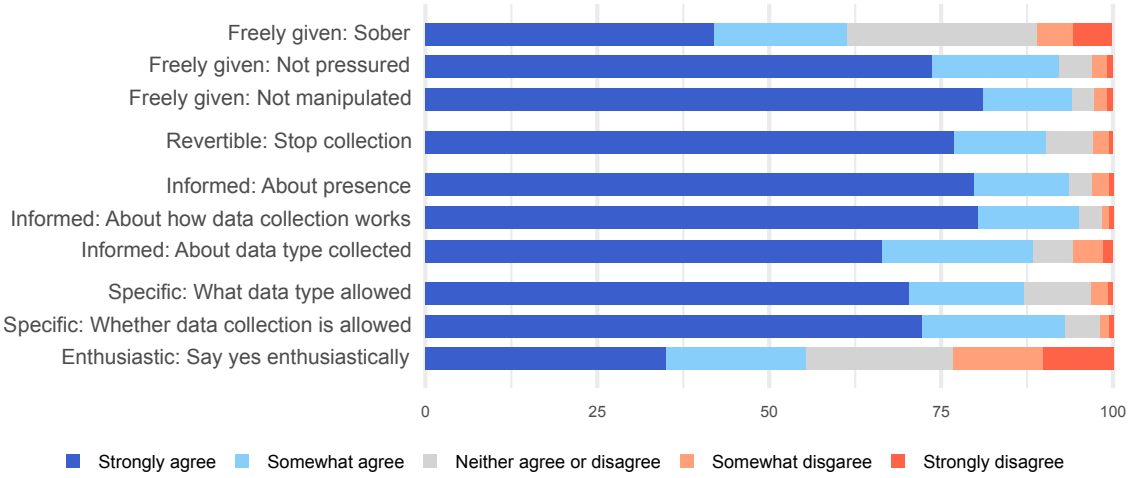

Figure 3: Participants rated the extent to which they agreed or disagreed that each of the above consent facets is important. For all consent facets, the majority of participants at least somewhat agreed that it is important.

freely given was relevant to their ratings thought process. P54, for example, explained why they reduced their rating from 6 to 2 for *plumber works near smart speaker* vignette in which the *freely given* facet of an incidental user – Seth's – consent was eroded: *"I think Seth being pressured into being around it is wrong."*

Even though *revertible* did not stand out in the regression analysis, 5% of participants (18) mentioned revertability in their free responses. For example, P69 stated: *"its okay to record but you should be able to delete your data."* Similarly, even though *specific* did not stand out in regression results, 3 participants brought up the idea of consent being specific. For P309, *"If the person living in the home doesn't fully understand what is being recorded even if they are fine with it being there, it seems a bit a bit [sic] problematic."*

"Enthusiastic" and *"unburdensome"* were not mentioned often (by one and four participants respectively). However, 9% of participants (34) brought up the incidental user's comfort, and this theme emerged especially in participants' explanations of their score change when we had eroded the *enthusiastic* consent facet (17 of the 34). For example, in response to the incidental user not being enthusiastic in the *bedside camera in rental* vignette, P11 wrote *"Its not acceptable because shes uncomfortable with it."*

4.4 RQ3: Context affects the perceived importance of consent facets

We next ask when consent might be especially important. We answer this question by considering how vignette differences besides our consent manipulation lead to differences in participants' acceptability ratings.

Figure 4 shows how participants' baseline and revised acceptability ratings changed for each vignette. As expected, baseline ratings varied substantially (e.g., the *bedside camera in rental* vignette was viewed as less acceptable in the baseline than other vignettes), but we also note that the relative rating changes after consent erosion are not uniform across all vignettes. *Motion sensor in newlyweds' home* had the most drastic average rating change (-1.5) while *bedside camera in rental* saw the smallest (-0.2).

Our regression analysis suggests that the Device type and Relationship between the device owner and incidental user both had an effect on change in acceptability score. The motion sensor was associated with a -0.36 greater change in acceptability compared to all other devices, while the smart camera was associated with -0.35 greater change than the smart lock. The largest observable effect was the co-residents relationship; stories in which the incidental user was a resident were associated with a -0.68 greater change in acceptability as compared to stories about employer-employee or co-residents; inspection of the credible interview shows that this effect is consistently observable with a lower bound of -0.47. This provides evidence that, intuitively, performing non-consensual data collection within someone's own home was particularly unacceptable to participants. The employer-employee relationship is also consistently observable in comparison to host-guest with a weaker mean effect of -0.32 and a lower bound of -0.07.

Below, we provide results from qualitative coding that further convey how context affected perceptions of consent facets. These results support the regression results above and give insights about the influence of other vignette details.

4.4.1 Relationship. Regression analysis shows that for vignettes that depict co-resident relationships, eroding consent resulted in a significantly bigger rating shift than for vignettes where the incidental user is a guest or domestic worker; qualitative findings provide substantial additional nuance.

Several participants' explanations of their ratings mentioned that the closeness of the relationships we described had shaped their views; however, the directionality of this influence varied. Both having a close relationship and being strangers were cited as reasons to worry both less and more about consent erosion. For example, P34 wrote, *"I think this is very fair since Abigail does not know Heather personally, I see nothing wrong with this."* In contrast, P106 said, *"It*

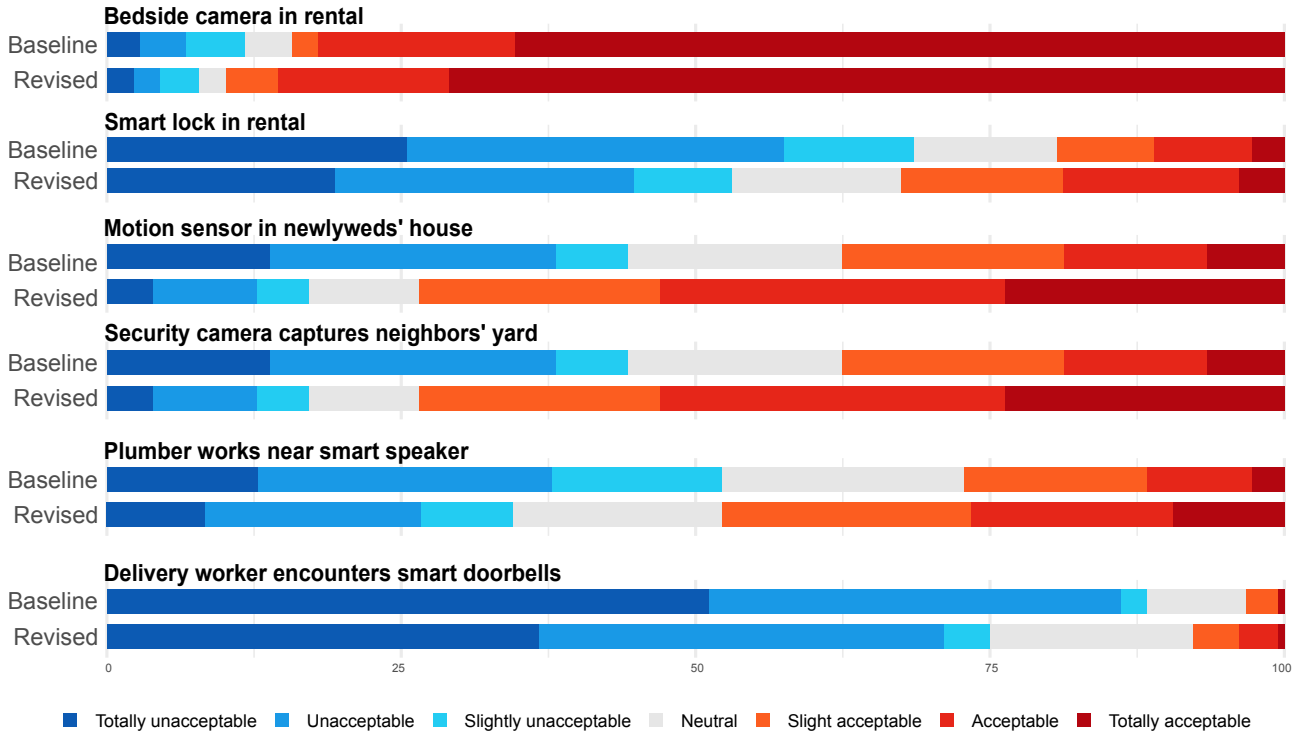

Figure 4: This figure shows participants' baseline and revised acceptability ratings split based on which vignette they were shown. The *bedside camera in rental* vignette tended to be seen as especially unacceptable in both the baseline and revised ratings. *Motion sensor in newlyweds' home* had the largest shift in between baseline and revised ratings.

is not appropriate to record strangers in privacy" (i.e., emphasizing that the incidental user and device owner were strangers).

We also saw evidence that the closeness of a relationship may not be sufficient for capturing views and of differing assumptions about what constitutes a close relationship. For example, P208 emphasized the nature of the relationship in our *plumber works near smart speaker* vignette; they did not revise their acceptability rating after consent erosion and wrote: *"[The plumber] works inside other people's homes. He can't expect privacy during his work. If being seen or heard during his work bothers him, he should seek a different line of work."* P18 emphasized the longevity of the plumber working with this client in our vignette: *"He has been doing work for 10 years so he is a trusted hired worker."* The *longevity* and *nature* of relationships may influence the closeness of the relationship but may also have their own separate effects on views about consent in smart homes.

4.4.2 Device type and data type. Device type correlated with significant differences in the amount of impact eroding consent had in our regression analysis. There was a bigger change in acceptability rating for vignettes with motion sensors compared to all other types of devices, for vignettes with speakers compared to smart cameras or smart locks, and for vignettes with smart cameras compared to those with smart locks. 40% of participants (143) also mentioned the data type or device type in their explanations. Video and audio recordings seemed more alarming to participants, whereas door lock status and motion sensor data were often dismissed. For example, P5 explained why they felt consent was unimportant for smart locks: *"I think it's fine if it's just a lock, and not recording pictures or voices,"* and P124 was similarly unbothered by motion sensors: *"... only a motion sensor, would not phase [sic] me. If it were a camera that would be different."*

Surprisingly, vignettes with motion sensors had a relatively large acceptability rating change; however, this might be due to confounding factors. For example, the *bedside camera in rental* vignette had an especially low baseline that may have created a floor effect and limited the capacity for cameras to emerge as having a large impact on rating changes. Additionally, *motion sensor in newlyweds' home* was the only vignette with a motion sensor while featuring a more intimate relationship. Therefore, our ability to interpret motion sensors' effects might be limited as the more intimate relationship may have had a significant impact on baseline ratings.

4.4.3 Other factors. In addition to Device and Relationship type, which we intentionally varied, other factors embedded in the vignettes may have affected participants' views. Specifically, participants commented on the importance of devices' *location* and their underlying expectations which were shaped by societal *norms*.

25% of participants (89) differentiated public versus private areas. Consent tended to be less important in public areas (e.g., outside) and more important in private places (e.g., bedrooms). For example, P209 wrote: *"Renters deserve complete privacy in their bedrooms.*

They can maybe be filmed on the outside of the apartment for security purposes, but in the bedroom they shouldn't be filmed."

13% of participants (47) mentioned norms or expectations, generally suggesting that more normal data collection practices are more acceptable. For example, P332 explained why eroding the *informed* consent facet was irrelevant to their rating: *"I can honestly think of no reason why that would be less than totally acceptable to record video and audio from your doorbell. I think most people are now aware of the smart doorbells that so many people have."*

4.5 RQ4: Responsibility for obtaining consent

With an eye toward recommending appropriate solutions for improving the state of consent in smart homes, the final part of our study asks how the responsibility to obtain consent should be divided. We presented participants with a brief description unrelated to our vignette stories that illustrated the relationship of relevant stakeholders (i.e., device owners, incidental users, and device manufacturers). For each of the relevant stakeholders, participants rated the extent to which each group is responsible for obtaining consent. Ratings were on a 4-point scale from *not responsible* to *very responsible* (see Figure 5). Participants were free to specify more parties they find responsible in the form of free response answers.

4.5.1 Which stakeholders are responsible? 78% of participants (280) felt the device owner was very responsible, and only 14 participants (4%) felt the device owner had no responsibility to obtain consent. In contrast, only 3% of participants (10) rated incidental users as being very responsible for obtaining consent, and over 81% (290 participants) felt that the incidental user was not responsible. No clear consensus emerged in participants' responses about device manufacturers' responsibility for ensuring that consent is obtained before a device collects data about incidental users; responses to this question were split relatively evenly between finding manufacturers very, somewhat, a little, or not responsible (102, 62, 60, 115 participants, respectively).

Perhaps surprisingly, the way that participants rated responsibility did not always "add up" as one might expect; that is, some participants rated multiple stakeholders as holding substantial responsibility for obtaining consent. For example, 18% of participants (66 people) rated both device owners and manufacturers as very responsible, and another 14% (50 participants) rated device owners as very responsible and manufacturers as somewhat responsible.

Although participants could indicate that they "don't know" how much responsibility a particular stakeholder should bear, participants rarely used this option. Only 9% of participants (34) expressed uncertainty about any stakeholder and despite the lack of consensus for how much responsibility they should have, only 4% of participants (14) expressed uncertainty about to what degree device manufacturers are responsible.

4.5.2 Why are these stakeholders responsible (or not)? Above, we described *who* participants felt was responsible for gathering consent; we now consider how their free-response answers reflect *why* they feel this way and *what* responsibilities participants assign to each stakeholder.

Device owners When participants found device owners to be responsible, they most often explained that the owners are responsible because they are the ones who make decisions about purchases, ownership, or placement of devices (147 participants, 47%), or because they are the ones with knowledge about the devices (15 participants, 4%). For example, P32 wrote, *"consent should be the person who OWNS the device's responsibility because it was their choice to get it,"* and P345 explained, *"[the device owner] decides how to use it so no one else is responsible."* Further, several participants (7) emphasized that ignorance of how devices work does not absolve device owners of responsibility for obtaining consent; knowing about their own devices' capabilities and the fact that they collect data is the responsibility of device owners.

Connecting to our study's focus on multi-faceted consent, a total of 13% participants' (47) responses emphasized the *informed* consent facet. 3% of participants (10) wrote that owners are responsible because they did not inform the incidental users of the devices – an assumption that did not align with this survey question but may have carried over from earlier parts of the survey or participants' real-world experiences; and 12% of participants (42) wrote that the owners should inform incidental users about the data collection.

Incidental users 3% of participants (10) wrote that incidental users are responsible because they have control over their own actions, for example, they *"can leave the situation if needed"* (P171), *"should ask if there are devices they need to know about"* (P18), or *"could avoid being the Camera range"* (P337). We note that taking these actions would require an incidental user to be *informed* about or otherwise aware of devices. These participants may see this responsibility as conditional upon awareness or may be building on assumptions about consent that our study suggests are unreliable – recall from Section 4.1 that 48% of participants had a real-world experience in which they were not *informed* about the data collection process of someone else's device. To this end, 1% of participants (2) believed that incidental users should anticipate or know about the data collection, because smart home devices are common. P162 summed up these sentiments in this comment: *"I expect most delivery drivers know that people have doorbell cameras and that they (the drivers) have no control over them."*

Device manufacturers As described above, participants' opinions regarding whether device manufacturers are responsible for obtaining consent to smart home devices' data collection were split. These mixed perspectives also emerge in free-response explanations. 7% of participants (24) wrote that the manufacturers are not responsible since they have no control over how the owners use their products. P345 said that *"just because [the device manufacturer] supplies the smart speaker, they have no control over how the buyer uses it."* This is consistent with participants finding device owners responsible because they have control over the devices – here, a similar mentality suggests that manufacturers are not responsible because they have no control over devices after they are sold. Even though manufacturers lose control once devices are sold, 3% of participants (10) stated that they are still responsible since they are aware of their products' capabilities and how they might be used (e.g to collect data without consent).

Other participants pointed out that manufacturers *do* have some control and felt this made them at least somewhat responsible. 8% of participants (29) wrote that the manufacturers are responsible because they enable owners by providing the devices and services.

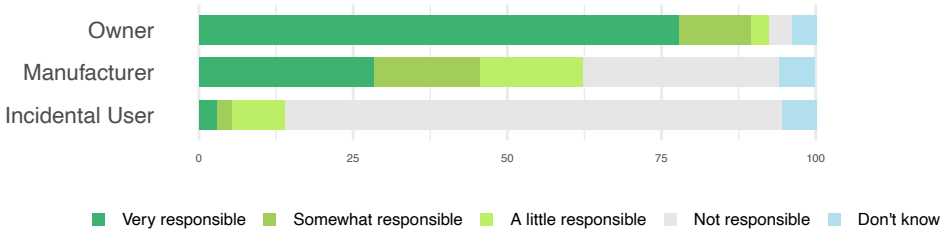

Figure 5: Participants indicated how much responsibility device owners, manufacturers, and incidental users had if consent was not obtained before data was collected. Overwhelmingly, participants saw device owners as responsible and incidental users as not responsible; however, they had differing views about manufacturers.

Without their devices, the owners would not be able to collect data from incidental users. *"The company is mainly responsible, they created the device ... the manufacturer is fully responsible for design flaws"* (P47). 3% of participants (9) wrote that manufacturers are responsible for designing better products, such as *"making sure people can easily tell if they are being recorded"* (P20), *"have systems in place to prevent unauthorized recording"*(P189), or *"make their software not collect data of other people"* (P154). 1 participant listed *"Salesman of device"* (P330) as responsible in the free response answer. 6% of participants (21) felt manufacturers have the responsibility to inform incidental users, e.g., P108 wrote that the manufacturer *"must warn about what data is collected by its devices."*

Other stakeholders Some participants wrote about other stakeholders they thought had some responsibility for ensuring there is consent. Three indicated that lawmakers are responsible to varying extents, saying that lawmakers are *"slightly responsible because they could make [device manufacturers] not collect data on people who didn't consent"* (P87), or *"largely responsible due to allowing companies to create systems that can collect data without consent"* (P184). Two participants stated that *"everyone"*(P338) or *"society"* (P163) was responsible. P163 stated that, *"...[the manufacturer] is filling a demand for recording devices. The demand itself exists because we've built a surveillance society where crime is rampant and privacy has been sacrificed so we can pretend we're deterring it."*

5 DISCUSSION AND CONCLUSIONS

Our study provides nuanced insights that advance our understanding of the importance of consent in smart homes and how we could move toward more appropriate consent practices in these contexts. Here, we summarize our key findings, interpret our findings with an eye toward legal and design implications, and discuss future research directions that could further advance our understanding of smart home data collection preferences and best practices.

5.1 Multi-faceted consent is needed in smart homes

Our study demonstrates that current consent practices in smart homes are insufficient; if we are to make suitable improvements, we should adopt a multi-faceted lens for data collection consent. First, while prior work has demonstrated how common it is for people to be incidental users (or bystanders) in smart homes [20], our study additionally shows that non-consensual experiences in smart homes are common; 84% of participants in our study had experienced a situation where at least one consent facet was absent. This may even be a low estimate considering that some participants may not even realize that they were never *informed* about smart home data collection. Moreover, almost half of the participants had experienced a real-world situation in which they were not informed about a smart home device while fewer than 10% had experiences in which their consent was not freely given. Informed may have emerged as especially impactful in our acceptability rating analysis despite aligning with prior experiences; that is, we may be underestimating the value participants placed on the informed consent facet

Like prior studies [3, 55, 85, 88], we find that it is especially important for incidental users to be *informed*. However, we have also shown that consent facets such as *freely given* may be just as important; we found that eroding *freely given* had greater negative impact on participants' acceptability ratings than eroding *informed*. As we will discuss in Sections 5.2 and 5.3, addressing lack of *informed* will not necessarily solve problems related to other consent facets. Expectations and preferences about each consent facet also seem to depend on contextual factors such as the Device type involved in data collection and the Relationship between the device owner and incidental user. Thus, multi-(consent)-faceted solutions geared toward a wide variety of smart home situations are needed.

While affirmative consent theory has been suggested as a generative theoretical foundation to imagine consentful sociotechnical systems [34], our results suggest affirmative consent specific facet, *enthusiastic*, may not be the most suitable for smart homes. Although almost 25% of participants somewhat or strongly disagreed that *enthusiastic* consent is important, many used the term "(un)comfortable" to explain their revised acceptability ratings. Like their non-smart counterparts, smart home devices such as door locks, ovens, and toilets are not necessarily intended to rouse excitement or enthusiasm, but rather to blend into a slightly easier everyday life. While there may be times when someone is actively *enthusiastic* about the presence or design of a household item, we suggest that *comfortable* may be a more appropriate expectation in the (smart) home setting and, thus, more appropriate language to describe this consent facet.

Table 6: Our recommendations for how each of various stakeholder groups could help create more consentful smart homes.

Stakeholders	Recommendations
Policymakers	Regulations that serve as sources of law to remove data not freely given (*Freely given, Revertible*) Regulations that mandate data deletion should be easy to request (*Unburdensome*)
Manufacturer	Features that inform incidental users better, e.g. features that remind owners to inform about the devices, features that automatically inform incidental users, features that streamline data collection consent discussion into pre-existing communication channels (*Informed*) Features that make data deletion easier, e.g. Automatically delete voices that do not match voice profiles, features that streamline data collection consent discussion into pre-existing communication channels (*Revertible*, *Unburdensome*)
Owner and users	Accommodating attitudes toward data collection-related request, e.g. ex-ante communication that allows incidental users to strategize (*Freely given*, *Informed*), express genuine support toward any data deletion request (*Revertible*)

5.2 Rethinking consent in smart homes

Having established that consent improvements are needed in smart homes, we now shift to a discussion of how our results lead to specific recommendations to accomplish this (Table 6).

Updating laws and policies While some existing laws and policies already incorporate several consent facets we studied, it is vital to establish regulations specifically for smart homes. Our results can serve as an initial guide for what lawmakers and technology creators should focus on. Informed by our insights regarding the importance of *freely given*, policymakers should establish legal frameworks that ensure that incidental users, especially those in more vulnerable situations, are not pressured into accepting unfair data collection agreements such as by having a legal basis to make data deletion claims. CCPA is the first regulation to grant the "right to delete," however, it has been reported that it is hard to make the actual requests as the process is tedious and complicated [84]. The Current solution to combat the obstacles of data deletion is to delegate the requests to authorized agents. Policymakers should continue their efforts toward *unburdensome* and *revertible* solutions as regulation empowers incidental users to make grounded claims.

Redesigning devices with consent in mind Prior work already suggested ways that smart home device manufacturers can offer better security and privacy to end-users [90]; our findings emphasize the importance of broadening more of these efforts to include incidental users and additional consent facets. For example, there is substantial ongoing work to improve awareness of smart home devices (i.e., improve upon the *informed* consent facet) [28, 64, 69, 77, 82]. Merely being aware of smart home devices is insufficient. Our finding about the prevalence of being *informed* being absent in so many participants' real-world smart home device encounters demonstrates that this is not yet solved. Future smart home systems should work toward informing incidental users better, such as features that automatically inform incidental users, or ecosystems that streamline data collection consent discussion into pre-existing communication channels. Additionally, some manufacturers now offer straightforward data deletion for device owners (i.e., deliver on the *revertible* consent facet) [6]; this type of capability could also be modified to suit incidental users such as by automatically deleting queries from unknown voice profiles or voice match. Along with this, other novel device features might be able to help reduce social pressures, re-balance power differences, or promote an *unburdensome* consent process. For example, devices could monitor nearby incidental users and offer them a streamlined consent-gathering channel that does not need to go through the device owners to.

Shifting community and societal behaviors Policymakers may seem the most well-positioned to push for smart home regulation. However, creating more consentful smart home environment also depends on device owners and community members to shape the overall smart home environment. To foster consentful smart homes, here we advocate that device owners should also take proactive efforts. The following suggestions are aimed to reduce social pressure for incidental users and make consent *freely given*, *informed*, *specific*, and other facets we found were important to participants. For example, a device owner could begin telling incidental users about smart home devices before they arrive (*informed*), pointing them out upon arrival (*informed*), showing them how the devices work (*specific*), directly asking if they are okay with devices being turned on while offering extra reassurances that it is okay to say no (*freely given*), or they could even turn devices off when inviting someone over (i.e., establish an opt-in rather than opt-out policy). Incidental users could (for their own sake or the sake of broader social change) more frequently request that a device be moved or turned off when they are nearby, despite the existing social pressures not to do so. While the suggested actions could be socially (and potentially professionally) risky [4, 11, 88], challenging or intentionally reestablishing norms could be quite powerful, especially within small communities and friend groups. Both device owners and incidental users can benefit from more effective and formalized ways to communicate consent. Researchers have started exploring how tangible interfaces can be beneficial to consent communication, such as control boards, physical objects, and other mechanisms to create awareness of ongoing data collection [21, 82, 86].

5.3 Future research directions

Our findings reveal new directions to help further improve consent practices in the challenging and dynamic setting of smart homes. The importance of consent and the challenges of establishing certain consent facets, such as *freely given* may be especially applicable

to vulnerable groups such as domestic workers [12–14]. Since *freely given* is dependent on social dynamics, future work might first systematically understand the relationship between consent decisions, preferences, and various relationships between device owners and incidental users. Researchers can also explore mechanisms to facilitate incidental users to make authentic consent decisions instead of having data collection forced upon them. These could be *ex-ante* notices before arriving on site where incidental users would be faced with social pressure or having the consent decisions handled by a third-party platform, so the consent decisions are anonymous to the device owners (or other sources of pressure). Follow-up studies could also utilize alternative consent manipulations to improve our understanding of the role each consent facet plays in smart homes (e.g., emphasizing *presence* of a consent facet rather than eroding it). Such follow-up studies would also provide opportunities to study the extent to which it is appropriate to consider *comfortableness* as a consent facet in smart homes (e.g., as language in laws and policies or for guiding device creators' efforts).

ACKNOWLEDGMENTS

We thank our amazing colleagues in the Cobb Research On Privacy & Security (CROPS) Lab for their feedback and support. We thank Kentrell Ownes and Lucy Simko for helping us pilot our early study designs. We thank Vinay Koshy for his comments and suggestions throughout all iterations. This research is in part supported by the SPLICE research group under the National Science Foundation (NSF) SaTC Frontiers program award number 1955228. The findings and discussions are those of the authors and do not represent NSF.

REFERENCES

[1] 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, CSCW (2020), 1–28.

[2] Wael S Albayaydh and Ivan Flechais. 2022. Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI'22)*. Association for Computing Machinery, New York, NY, USA, Article 446, 24 pages. https://doi.org/10.1145/3491102.3502097

[3] Tejasvi Alladi, Vinay Chamola, Biplab Sikdar, and Kim-Kwang Raymond Choo. 2020. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine* 9, 2 (2020), 17–25.

[4] 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 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI'23)*. Association for Computing Machinery, New York, NY, USA, Article 67, 27 pages. https://doi.org/10.1145/3544548.3581360

[5] 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.

[6] Amazon. 2011. Delete Alexa Voice Recordings Automatically. https://www.amazon.com/gp/help/customer/display.html?nodeId=G68KUKTXN92WY3C3

[7] Hany F Atlam and Gary B Wills. 2020. IoT security, privacy, safety and ethics. In *Digital twin technologies and smart cities*. Springer, Cham, Switzerland, 123–149.

[8] Christiane Atzmüller and Peter M Steiner. 2010. Experimental vignette studies in survey research. *Methodology* 6, 3 (2010), 128—-138.

[9] Solon Barocas and Helen Nissenbaum. 2014. Big data's end run around procedural privacy protections. *Commun. ACM* 57, 11 (2014), 31–33.

[10] Carlos Bermejo Fernandez, Dimitris Chatzopoulos, Dimitrios Papadopoulos, and Pan Hui. 2021. This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW (2021), 1–22.

[11] 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 *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 687–706.

[12] Julia Bernd, Ruba Abu-Salma, and Alisa Frik. 2020. Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance. In *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*. USENIX Association, "".

[13] Julia Bernd, Alisa Frik, Maritza Johnson, and Nathan Malkin. 2019. Smart Home Bystanders: Further Complexifying a Complex Context. In *Proceedings of the 2nd Symposium on Applications of Contextual Integrity*.

[14] Nellie Bowles. 2018. Thermostats, locks and lights: Digital Tools of domestic abuse. *The New York Times* (23 Jun 2018). Available at: https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html (Accessed: July 16th, 2023).

[15] Stephen Breen, Karim Ouazzane, and Preeti Patel. 2020. GDPR: Is your consent valid? *Business Information Review* 37, 1 (2020), 19–24.

[16] Robert L Brennan and Dale J Prediger. 1981. Coefficient kappa: Some uses, misuses, and alternatives. *Educational and psychological measurement* 41, 3 (1981), 687–699.

[17] Rachel Cericola. 2022. These Smart Home Devices Can Enhance Independence for People With Disabilities and Mobility Needs. *Wirecutter* (29 Apr 2022). Available at: https://www.nytimes.com/wirecutter/reviews/best-assistive-smart-home-technology-for-disabled(Accessed: July 16th, 2023).

[18] Rachel Cericola. 2023. The Best Smart Home Devices to Help Seniors Age in Places. *Wirecutter* (30 Mar 2023). Available at: https://www.nytimes.com/wirecutter/reviews/smart-home-for-seniors/ (Accessed: July 16th, 2023).

[19] Chola Chhetri and Vivian Genaro Motti. 2022. User-Centric Privacy Controls for Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW (2022), 1–36.

[20] 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* 4 (2021), 54–75.

[21] 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* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 74, 13 pages. https://doi.org/10.1145/3546155.3546640

[22] Yang Dong. 2021. Biometric Information Privacy Act: Statutes, Litigation, and Future. *Academic Journal of Humanities & Social Sciences* 4, 1 (2021), 19–23.

[23] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices. *IEEE Security & Privacy* 20, 2 (2021), 31–39.

[24] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI'19)*. Association for Computing Machinery, New York, NY, USA, 1–12.

[25] eSafety Commissioner. 2023. Consent. https://www.esafety.gov.au/key-topics/staying-safe/consent.

[26] Matthias Fassl, Lea Theresa Gröber, and Katharina Krombholz. 2021. Stop the consent theater. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–7.

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

[28] Tomas Gecevicius, Yaliang Chuang, and Jingrui An. 2021. Smart ARbnb: Smart home interface for Airbnb with augmented reality and visible light communication. In *Proceedings of the 2021 Workshops on Computer Human Interaction in IoT Applications co-located with the International Conference on Embedded Wireless Systems and Networks (EWSN 2021) and the 13th ACM SIGCHI Symposium on Engineering Interactive Computing Systems(EICS 2021)*.

[29] Julie Haney, Yasemin Acar, and Susanne Furman. 2021. "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 411–428.

[30] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things(IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 255–272.

[31] Tobias Heer, Oscar Garcia-Morchon, René Hummen, Sye Loong Keoh, Sandeep S Kumar, and Klaus Wehrle. 2011. Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications* 61, 3 (2011), 527–542.

[32] Dana Holmstrand. 2022. A Haunted (Smart) House: Smart Home Devices as Tools of Harassment and Abuse. *Georgiatown Law Technology Review* 223, 6 (2022), 223–247.

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

Systems (CHI'20). Association for Computing Machinery, New York, NY, USA, 1–13.

[34] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S Ackerman, and Eric Gilbert. 2021. Yes: Affirmative Consent as a Theoretical Framework for Understanding and Imagining Social Platforms. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)*. Association for Computing Machinery, New York, NY, USA, 1–18.

[35] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling multi-user controls in smart home devices. In *Proceedings of the 2017 workshop on internet of things security and privacy*. Association for Computing Machinery, New York, NY, USA, 49–54.

[36] Matthew Kay, Gregory L. Nelson, and Eric B. Hekler. 2016. Researcher-Centered Design of Statistics: Why Bayesian Statistics Better Fit the Culture and Incentives of HCI. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA). Association for Computing Machinery, New York, NY, USA, 4521–4532. https://doi.org/10.1145/2858036.2858465

[37] Jason Kelley and Matthew Guariglia. 2022. Ring Reveals They Give Videos to Police Without User Consent or a Warrant. https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant.

[38] 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 *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)*. Association for Computing Machinery, New York, NY, USA, 1–14.

[39] Udo Kuckartz and Stefan Rädiker. 2019. *Analyzing qualitative data with MAXQDA*. Springer, Cham, Switzerland.

[40] 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, CSCW (2018), 1–31.

[41] Una Lee and Dann Toliver. 2017. Building Consentful Tech. http://www.consentfultech.io/wp-content/uploads/2019/10/Building-Consentful-Tech.pdf.

[42] California State Legislature. 2018. California Consumer Privacy Act of 2018. In *California Civil Code*. California State Legislature, Part 4 of Division 3 of the Civil Code.

[43] Engin Leloglu. 2016. A review of security concerns in Internet of Things. *Journal of Computer and Communications* 5, 1 (2016), 121–136.

[44] Jessica Lis. 2021. Smart Home Forecast 2021. https://www.insiderintelligence.com/content/smart-home-forecast-2021.

[45] Ewa Luger and Tom Rodden. 2013. An informed view on consent for UbiComp. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. Association for Computing Machinery, New York, NY, USA, 529–538.

[46] Ewa Luger and Tom Rodden. 2014. Sustaining consent through agency: a framework for future development. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. Association for Computing Machinery, New York, NY, USA, 659–664.

[47] Dominique Machuletz and Rainer Böhme. 2020. Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies* 2 (2020), 481–498.

[48] Dominique Makowski, Mattan S Ben-Shachar, and Daniel Lüdecke. 2019. bayestestR: Describing effects and their uncertainty, existence and significance within the Bayesian framework. *Journal of Open Source Software* 4, 40 (2019), 1541.

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

[50] 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 *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. Association for Computing Machinery, New York, NY, USA, 1–11.

[51] Oriana McDonough. 2019. A Bystander's Dilemma: Participatory Design Study of Privacy Expectations for Smart Home Devices. https://surface.syr.edu/honors_capstone/1085/. *Syracuse University Honors Program Capstone Projects (May 2019* (2019).

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

[53] Michael McMahon. 2020. Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts. *St. Louis ULJ* 65 (2020), 897.

[54] Sayeed Mehrjerdian. 2019. Smart Devices for People With Disabilities. https://www.iaccess.life/useful-smart-home-devices-for-people-with-disabilities/.

[55] Nicole Meng, Dilara Keküllüoğlu, and Kami Vaniea. 2021. Owning and sharing: Privacy perceptions of smart speaker users. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW (2021), 1–29.

[56] Angela Moscaritolo. 2022. The Best Smart Home Devices for 2022. https://www.pcmag.com/picks/the-best-smart-home-devices.

[57] 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 *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 399–412.

[58] Josef Nguyen and Bonnie Ruberg. 2020. Challenges of designing consent: Consent mechanics in video games as models for interactive user agency. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI'20)*. Association for Computing Machinery, New York, NY, USA, 1–13.

[59] State of California Department of Justice. 2023. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa.

[60] ACLU of Illinois. 2008. Biometric Information Privacy Act (BIPA). https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipae.

[61] Council of the European Union. 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council*. https://data.europa.eu/eli/reg/2016/679/oj

[62] Stanislaw Piasecki and Jiahong Chen. 2022. Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law* 12, 2 (01 2022), 113–131.

[63] Eugenia Politou, Efthimios Alepis, and Constantinos Patsakis. 2018. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of cybersecurity* 4, 1 (2018), tyy001.

[64] Sarah Prange, Ceenu George, and Florian Alt. 2021. Design considerations for usable authentication in smart homes. In *Mensch und Computer 2021*. Association for Computing Machinery, New York, NY, USA, 311–324.

[65] David Priest, Rich Brown, Ry Crist, and Molly Price. 2022. Best Smart Home Devices of 2022. https://www.cnet.com/home/smart-home/best-smart-home-devices/.

[66] R Core Team. 2013. R: A language and environment for statistical computing. (2013).

[67] Mark Raymond. 2023. Usage and Buying Trends in Smart Home Devices: GoodFirms Research. https://www.goodfirms.co/resources/buying-smart-home-devices-statistics.

[68] Samantha Reig, Elizabeth Jeanne Carter, Lynn Kirabo, Terrence Fong, Aaron Steinfeld, and Jodi Forlizzi. 2021. Smart Home Agents and Devices of Today and Tomorrow: Surveying Use and Desires. In *Proceedings of the 9th International Conference on Human-Agent Interaction*. Association for Computing Machinery, New York, NY, USA, 300–304.

[69] Ring. 2021. Motion Warning Information. https://support.ring.com/hc/en-us/articles/360048674751-Motion-Warning-Information.

[70] Rowena Rodrigues, David Barnard-Wills, Paul De Hert, and Vagelis Papakonstantinou. 2016. The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. *International Review of Law, Computers & Technology* 30, 3 (2016), 248–270.

[71] Rstan. 2023. RStan: the R interface to Stan. https://mc-stan.org/users/interfaces/rstan.

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

[73] 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)*. USENIX Association, Ottawa, 1–17.

[74] Bart W Schermer, Bart Custers, and Simone Van der Hof. 2014. The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology* 16, 2 (2014), 171–182.

[75] Deepika Singh, Ismini Psychoula, Johannes Kropf, Sten Hanke, and Andreas Holzinger. 2018. Users' perceptions and attitudes towards smart home technologies. In *Smart Homes and Health Telematics, Designing a Better Future: Urban Assisted Living: 16th International Conference, ICOST 2018, Singapore, Singapore, July 10-12, 2018, Proceedings 16*. Springer, Springer International Publishing, Cham, 203–214.

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

[77] 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 *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI'20)*. Association for Computing Machinery, New York, NY, USA, 1–13.

[78] Peter M Steiner, Christiane Atzmüller, and Dan Su. 2016. Designing valid and reliable vignette experiments for survey research: A case study on the fair gender income gap. *Journal of Methods and Measurement in the Social Sciences* 7, 2 (2016), 52–94.

[79] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. 2023. "It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association,

Anaheim, CA, 105–122.
[80] Yolande Strengers, Jathan Sadowski, Zhuying Li, Anna Shimshak, and Florian 'Floyd' Mueller. 2021. What Can HCI Learn from Sexual Consent? A Feminist Process of Embodied Consent for Interactions with Emerging Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)*. Association for Computing Machinery, New York, NY, USA, 1–13.
[81] Security.org Team. 2021. Smart Home Consumer Trends and Shopping Insights: 2021. https://www.security.org/smart-home/consumer-shopping-insights/.
[82] 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 *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI'22)*. Association for Computing Machinery, New York, NY, USA, 1–13.
[83] 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 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212
[84] Kaveh Waddell. 2022. How 'Authorized Agents' Plan to Make It Easier to Delete Your Online Data. https://www.consumerreports.org/electronics/privacy/authorized-agents-plan-to-make-it-easier-to-delete-your-data-a8655835448/.
[85] Maximiliane Windl and Sven Mayer. 2022. The Skewed Privacy Concerns of Bystanders in Smart Environments. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 184 (sep 2022), 21 pages. https://doi.org/10.1145/3546719
[86] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. 2023. Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 70, 16 pages. https://doi.org/10.1145/3544548.3581167
[87] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428
[88] 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.
[89] Ammar Younas and Bakhodir Tohir ogli Mirzaraimov. 2021. To What Extent are Consumers Harmed in the Digital Market from the Perspective of the GDPR? *International Journal of Multidisciplinary Research and Analysis* 4, 8 (2021), 1187–1192.
[90] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng
[91] 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 (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

A RECRUITMENT MATERIALS

The study was advertised under the title, "Seeking participants for a study on smart home devices experiences" on Prolific. The study was described as follows:

> This research aims to understand people's attitudes for and experiences with smart home devices. This study includes a single survey that has three sections. In the first section, you will read three smart home stories and answer the questions related to the stories. In the second section, you will be asked how you feel about smart home devices in general. The survey will conclude with a set of demographic questions. Participants don't need to be owners of any smart home devices. Each participant will be rewarded $2.75 via Prolific.co for participation. If you would like to participate in the study, please open the survey link below. If you have any questions, feel free to email [Researcher name redacted for review] at [Email address redacted for review].

B SURVEY INSTRUMENT

Here we include an example of the survey that was shown to participants, with Vignette Set A (see Figure 3). In our example here, we erode *freely given*, *informed*, and *revertible*. The actual survey implementation randomized which consent facets were eroded. Answer choices for each question are shown in square brackets and italicized after each question. Red text in this section was not shown to participants but is included to guide the reader. The survey concluded with demographic questions.

Survey introduction

In this survey, we will be asking questions related to smart home devices. There are no right or wrong answers. Please feel comfortable to answer your honest opinion. The survey consists of three parts: Section 1: Read and respond to three short stories about smart home devices. Section 2: Answer general questions about smart home devices. Section 3: Provide demographic information. There are many different smart home devices with various features. Below are some examples of smart home devices we might ask you about in the survey. We are including pictures to help you contextualize the questions [2].

Section 1: Vignettes

Read the following story about two people interacting with a smart home device, and then answer the questions below.

> This story is about Vincent and Lewis. Vincent is a delivery driver. He has been delivering packages in the same residential areas for a little over a year, including Lewis's house. Vincent normally works 7-9 hours per day. He does not know anyone personally from the neighborhoods where he works. Many of the houses are equipped with smart doorbells that record video and audio.

- How do you feel about the smart doorbells in this story recording video and audio? *[1 Totally unacceptable - 7 Totally acceptable]*
- Suppose you found out that Vincent felt pressured into being around the smart doorbells. How do you feel now? *[1 Totally unacceptable - 7 Totally acceptable]*
- Please explain your reasoning behind the answers above. If your rating changed with the added information, please elaborate on why. *[Free response]*

Read the following story about two people interacting with a smart home device, and then answer the questions below.

> This story is about Mike and Christina. Mike has been gardening for a couple of years now. Mike waters his front lawn every day and maintains the garden over the weekends. Christina is Mike's next door neighbor. They exchange friendly waves and occasionally chat informally about house maintenance. Christina has installed a security camera that records video and

[2]Pictures sources and credits: Smart speaker, Smart lock, Smart doorbell, Motion sensor, Security camera, Smart home hub

> audio. Even though the camera is pointed at her door, it also records video of Mike's yard and garden.

- How do you feel about the security camera in this story recording video and audio? *[1 Totally unacceptable - 7 Totally acceptable]*
- Suppose you found out that Mike was not informed about the data collection of the security camera. How do you feel now? *[1 Totally unacceptable - 7 Totally acceptable]*
- Please explain your reasoning behind the answers above. If your rating changed with the added information, please elaborate on why. *[Free response]*

Read the following story about two people interacting with a smart home device, and then answer the questions below.

> This story is about Darla and Chuck. Darla is staying in Chuck's short-term rental apartment for one night. Darla does not know Chuck personally. Chuck has a smart camera that records both video and audio on the bedside table.

- How do you feel about the smart camera in this story recording video and audio? *[1 Totally unacceptable - 7 Totally acceptable]*
- Suppose you found out that Darla could not delete the data captured by the smart camera. How do you feel now? *[1 Totally unacceptable - 7 Totally acceptable]*
- Please explain your reasoning behind the answers above. If your rating changed with the added information, please elaborate on why. *[Free response]*

Section 2: General questions

In the stories you read previously, we described specific situations in which smart home devices collected data [about someone who did not own or install the device]. While answering the questions below, please reflect on your thoughts in general about smart home data collection.

Jackie has a smart device made by IntelligentHome that collects data about Sam. To what extent each of the following group is responsible if consent is not obtained before a device collects data about Sam?

- Jackie *[1 Not responsible, 2 A little responsible, 3 Somewhat responsible, 4 Very responsible, Don't know]*
- IntelligentHome *[1 Not responsible, 2 A little responsible, 3 Somewhat responsible, 4 Very responsible, Don't know]*
- Sam *[1 Not responsible, 2 A little responsible, 3 Somewhat responsible, 4 Very responsible, Don't know]*
- Some one else *[1 Not responsible, 2 A little responsible, 3 Somewhat responsible, 4 Very responsible, Don't know]*
- Please use the space below if you would like to give additional explanations about your choices above. [Free response]

Consider a situation in which person A allows a smart home device to collect data about them.To what extent do you agree or disagree with the following statements? (Statements were randomly ordered.)

- It is important that person A is sober *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A does not feel pressured into allowing the data collection *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A is not manipulated into allowing the data collection *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A can stop the data collection process at any time *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A is informed about the presence of the smart device *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A is informed about how the smart device works *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A is informed about what data the smart device collects *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A can specify what they allow the data collection *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A is sure of whether they have allowed the data collection *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- It is important that person A says yes to data collection enthusiastically *[Strongly disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Strongly agree]*
- If there are any other factors that are important to you that you feel we should have asked about, please mention those here as well. *[Free response]*

Which of the following have you personally experienced when you were around someone else's smart home devices? Please select all that apply.

- *I was unable to delete data that someone else's smart home device(s) collected about me,*
- *I was not informed about the data collection process of someone else's smart home device(s),*
- *I was unenthusiastic about being around someone else's smart home device(s) that were collecting data about me,*
- *I was unable to describe specific details about the data someone else's smart home device(s) could or could not collect about me, such as what types of data they collected or when they collected the data,*
- *I was unable stop the data collection from someone else's smart home devices(s) easily,*
- *I was not sure whether I agreed to let someone else's smart home device(s) collect data about me,*
- *Others [Free response]*

Section 3: Personal

The following questions will help us understand if the stories you may have read in the previous part of the study are relevant to your personal experiences:

- Have you ever installed, configured, or owned a smart home device? *[No, Yes]*
- Have you ever interacted with a smart home device that is not yours (e.g., a display model at a store, someone else's place, or workplace)? *[No, Yes, I am not sure]*
- Do any of your neighbors have smart home devices outdoor? *[No; Yes, smart doorbell; Yes, smart camera; Yes, smart speaker; Yes, smart lock; Yes, other smart devices; I am not sure*
- Have you ever visited another house where there were smart home devices? *[No; Yes, smart doorbell; Yes, smart camera; Yes, smart speaker; Yes, smart lock; Yes, other smart devices; I am not sure*
- Have you ever stayed in a short term rental (e.g., VRBO or AirBnB)? *[No, Yes]*
- Are or have you ever been a domestic worker, such as babysitter, delivery person, plumber? *[No, Yes]*
- Have you ever had domestic workers working in your household, such as babysitter, delivery person, plumber? *[No, Yes]*
- This item was only shown to participants who indicated that they had stayed in a short term rental. During your stay in a short term rental (e.g., VRBO or AirBnB), have you ever seen or interacted with smart home devices in the rental? *[No; Yes, smart doorbell; Yes, smart camera; Yes, smart speaker; Yes, smart lock; Yes, other smart devices; I am not sure*
- This item was only shown to participants who indicated that they had been a domestic worker. In your capacity as a domestic worker have you ever seen or interacted with smart home devices? *[No; Yes, smart doorbell; Yes, smart camera; Yes, smart speaker; Yes, smart lock; Yes, other smart devices; I am not sure*
- Please use to space below for anything else you want to tell us, or feedback you want to give about the survey *[Free response]*

C CONSENT FACET DETAILS

Table 7 lists the facets, their origins, and the statements about the importance of the facets.

D FREQUENTIST LINEAR REGRESSION MODEL

A summary of our regression model in the Frequentist framework is shown in Table 8.

Both the Bayesian and the Frequentist models support the same conclusions for each and every comparison in the data. The estimates for each comparison are roughly equal, and each comparison that comes out significant ($p < 0.05$) has a 95% credible interval in the Bayesian posterior distribution where all change scores are below zero. The level of agreement between the two models is expected as we had no basis for setting an informative prior in our novel study paradigm.

E QUALITATIVE CODEBOOK

Table 9 shows the codebook we used for analyzing participants' free-response answers. The thick horizontal line divides codes applied to responses from different sections of the survey. Above the thick horizontal line are codes used on participants' explanations of their thought process for the Likert-scale baseline and revised acceptability ratings for vignettes (i.e., participants are represented up to three times in the frequency count in this table, since each participant saw three vignettes). Below the thick horizontal line are codes applied to responses to our question about who is responsible if consent is not obtained before data is collected in a generic smart home scenario.

Table 7: Consent facet details: which consent framework includes each facet and statements used in our survey to directly ask participants about the importance of each facet.

Consent Facet	Framework(s)	Statements about consent facet importance "It is important that person A ..."
Freely-given	Affirmative consent, Consentful technology, GDPR	- is sober, - does not feel pressured into allowing the data collection, - is not manipulated into allowing the data collection
Revertible	Affirmative consent, Consentful technology, GDPR	- can stop the data collection process at any time
Informed	Affirmative consent, Consentful technology, GDPR	- is informed about the presence of the smart device, - is informed about how the smart device works, - is informed about what data the smart device collects
Enthusiastic	Affirmative consent, Consentful technology	- says yes to data collection enthusiastically
Specific	Affirmative consent, Consentful technology	- can specify what they allow the data collection - is sure of whether they have allowed the data collection
Undurdensome	Affirmative consent, GDPR	We unintentionally omitted a statement for *unburdensome*

Table 8: Summary of Frequentist Linear Mixed Effects Regression Model. Significance is denoted by *** ($p < 0.001$), ** ($p < 0.01$), and * ($p < 0.05$), with '.' denoting results trending towards significance ($p < 0.1$).

Variable	Estimate	Std. Err.	t
Intercept	-0.761	0.044	-17.162 ***
Device Type (Reference Level = Smart Lock)			
Motion Sensor	-0.363	0.139	-2.606 **
Smart Speaker	-0.156	0.123	-1.271
Smart Camera	-0.348	0.101	-3.462 ***
Relationship (Reference Level = AirBnb Guest)			
Resident	-0.686	0.113	-6.057 ***
Employee	-0.321	0.129	-2.496 *
Consent Facet (Reference Level = Specific)			
Freely-Given	-0.720	0.107	-6.715 ***
Informed	-0.347	0.106	-3.267 **
Enthusiastic	-0.318	0.107	-2.956 **
Unburdensome	-0.222	0.114	-1.957 .
Revertible	-0.039	0.135	-0.290

Table 9: Codebook details: The codes and their parent groups.

Groups	Codes	Frequency
Resurfacing themes from prior work	Device type: just a device	116
	Norms: adhere or break	52
	Data type: just data type	81
	Location: public v. private	109
	Closeness: close v. stranger	25
Mention of consent/permission	Consent is not important	6
	Mentions permission and consent	1
	Mention permission only	15
	Mentions consent only	43
Mention of specific consent facets	Freely given	24
	Informed	125
	Revertible	19
	Enthusiastic	1
	Specific	3
	Unburdensome	7
	Discussion/None one way declaration	28
Manufacturers are responsible	They can foresee	10
	Their creation enables the user	29
Manufacturers are not responsible	They are not the ones using the device	24
Manufacturers' responsibility	Better design decision	9
	Informing efforts	21
Owners are responsible	Did not inform incidental user	10
	They know about the devices	15
	Have control over decisions	147
Owners' obligation	Should inform the incidental users	42
Incidental users are responsible	Agency	20
Incidental users' obligation	Should know about devices	7
Other stakeholders are responsible	Those who collect data	36
	Lawmaker, salesperson	5
Participants want more information about the situations		24