Exploring privacy implications of awareness and control mechanisms in smart home devices

Madiha Tabassum
University of North Carolina at Charlotte
Charlotte, North Carolina, USA
mtabassu@uncc.edu

Heather Lipford
University of North Carolina at Charlotte
Charlotte, North Carolina, USA
Heather.Lipford@uncc.edu

Abstract

Smart home users have a variety of controls they can use to configure their devices according to their preferences. However, it is unclear how people utilize these controls, what considerations they make, and the implications of those decisions for users' privacy. To address this gap, we have conducted two complimentary interview studies regarding the controls available for configuring, monitoring, and sharing collected information in two common smart home devices: a smart doorbell and a lock. We interviewed 21 non-owner participants in the lab and 18 owners of these devices over the phone. While both novice users and existing owners were primarily driven by desired functionality while setting up their devices, their configuration decisions impact what data gets collected and how that data and the device are used and shared. Our findings suggest a range of opportunities to improve the privacy-related features and support for smart home devices.

Keywords

Smart home, User controls, Privacy, Qualitative study

1 Introduction

Homes are becoming more connected with the widespread use of Internet of Things (IoT) devices. From lights to the doorbell, coffeemaker to the vacuum cleaner, different vendors are continuously releasing Internet-connected devices that are being rapidly adopted for automation and convenience. Despite the fast adoption, security and privacy issues surrounding these devices remain at the top of consumers' concerns in using smart home devices [5, 10].

Because of the widespread use and adoption of smart homes and pervasive concerns surrounding privacy, the research community has examined end-users' privacy expectations, perceptions, and concerns [11, 26, 39, 45, 47]. Researchers found that users are concerned about ubiquitous data collection, sharing, inference, and access-control in the smart home. In response to these concerns, multiple efforts have been made to provide users more awareness and control over their privacy in the smart home [19, 20, 46], with suggestions and guidelines for desired features such as data localization and disconnection from the Internet [44].

The way that smart home controls are designed and offered to users has implications on how end-users manage their privacy. For instance, a lack of usable and granular access controls leads to account sharing [16, 40]. However, studies found that some of the privacy controls (i.e., mute button and audio logs in smart speakers) developed to help users with their concerns are rarely used [29, 31], indicating a potential privacy paradox [38]. Hence, we believe it is important to understand how people use the controls available to them and what considerations they make while configuring and managing those controls. Understanding how end-users make their decisions will help us to identify the gaps between the perspectives of the end-users and the designers of these controls and the potential points of interventions to provide more support for privacy management.

Therefore, this paper aims to understand end-users' perceptions and use of different controls and how these considerations and available features shape their behaviors and implicate privacy in the smart home. We present the results of two semi-structured interview studies developed around the configuration, monitoring, and sharing features available in a smart doorbell and smart lock. We chose these two particular devices because they collect video data and provide physical access to the home, both of which have been found to be perceived as sensitive by users in prior research [39, 45]. We interviewed 21 non-owners in a lab-based study as they interacted with these devices, as well as conducted a separate interview with 18 owners of these devices over the phone. We aimed to understand:

- RQ1: How do end-users perceive the controls available for configuring, monitoring, and sharing a smart lock and doorbell? What considerations do end-users have when configuring and managing the smart lock and doorbell?
- RQ2: What are the privacy implications of users' decisions? What security and privacy behaviors (or lack thereof) do they exhibit to support those considerations and their implications?
- RQ3: What additional awareness and controls do users want to satisfy their needs in the smart home?

As expected, both owners and non-owners are mainly driven by functionality when configuring their smart home devices, yet their configuration decisions have implications on what and how the data get recorded, accessed, and shared. However, smart home device interfaces often lack transparency and feedback to inform users of the privacy implications of their decisions and support privacy management. The main contributions of our paper are:

- First, our study provides insight into how users employ the controls available to them for the smart doorbell and lock, and how that affects the privacy of the people surrounding these devices.

Proceedings on Privacy Enhancing Technologies 2023(1), 571–588

https://doi.org/10.56553/popets-2023-0033

- Second, we extend the prior literature on smart home privacy by identifying additional gaps between users' privacy needs and concerns, and available awareness and control mechanisms.
- Third, we identify a number of design improvements that could provide better privacy options and controls for end users while still meeting their functional goals.

2 Related work

2.1 Privacy in the smart home

Extensive research has been done in recent years examining privacy in the smart home from a user-centered perspective. Zeng et al. [45] and Tabassum et al. [39] interviewed end-users' regarding their mental models, perceptions, and concerns of their smart homes. They found that users mostly consider the functionality of the smart home products and have limited concerns over the possible privacy risks [47]. This limited concern is often influenced by their trust in different entities, and the notion that they have nothing to hide. Thus prior research indicates that users are often valuing the convenience they receive from their devices over the low privacy risks they perceive, a concept referred to as privacy calculus [18, 27]. As a result, users often lack the motivation to take any substantial mitigation actions to protect their privacy in the smart home [39, 45, 47]. In fact, Haney et al. found that users assign most of the responsibility of security and privacy of the smart home to the manufacturer and the government or other third parties [24]. Yet, security and privacy concerns are still one of the main adoption barriers of smart home devices [21, 29], and those with greater privacy concerns may be avoiding such devices altogether, and the potential benefits they could provide.

A number of survey studies have been conducted to get a more detailed view of end-users' privacy preferences and elicit existing privacy norms in the smart home [13, 14, 37]. Apthorpe et al. surveyed 1731 individuals to identify acceptable information flows in the smart home, including device type, data type, data recipient, and data collection conditions [13]. Abdi et al. followed a similar approach to identify acceptable information flows with a smart personal assistant [12]. They found that the recipient of the data is the most influencing factor in determining the acceptability of the information flow. Barbosa et al. have also conducted a contextual survey involving data type, purpose of data use, and different situational factors to elicit users' preferences. They found that smart home users are most uncomfortable when data is used for a purpose that is beyond the primary goal of providing convenience [14].

Several other studies specifically looked at privacy in the multi-user smart home [23, 26, 45]. They found power imbalances between the admin users who set up and maintain the devices and the other household members. The admin user has more access and control of the data and the functionality. Koshy et al. further explore this issue and found that admin users configure the devices to meet their needs first, and others mostly depend on them for the information and features of the device [28]. Such a lack of involvement creates the potential for abuse from the admin user [30, 35, 45].

Several other studies looked at the perspective of the non-household members, aka bystanders (visitors, neighbors, etc.) [17, 33, 43]. Mare et al. interviewed Airbnb hosts and guests and found tensions between them around data collection, especially by smart cameras, voice assistants, and motion sensors [33]. In a focus group and co-design study, Yao et al. found that bystander privacy perceptions are primarily influenced by perceived device utility, perceived social relationship, perceived trust, and length of stay [43]. Cobb et al. found that owners of smart home devices are willing to accommodate bystanders as long as they agree with their concerns. However, tension remains as the owners and the bystanders can have very different concerns [17].

While prior studies have examined smart home users' privacy concerns and perceptions of risks, there is still a gap in understanding the impact and use of the device interfaces themselves - the controls that the companion apps make available for configuration and access. We sought to address this gap by examining users' considerations and decisions with those controls, and the implications of those decisions for privacy.

2.2 Awareness, notice and control

Privacy notice and awareness are critical to inform users of the privacy issues and risks to help them make decisions. Multiple research efforts have examined ways to provide such awareness in the smart home context. Emami-Naeini et al. proposed an IoT Security and Privacy Label [20] to be placed on the package of any IoT device that contains all the key information regarding the device's data practices (e.g., data collection purposes, data storage location, etc.). Mozilla has created an online guide called 'privacy not included' where consumers can learn about the data practices and possible risks from different smart home and IoT devices, [9]. These would help existing users to assess their risk, and potential buyers can decide whether and which device to buy. Researchers have also proposed multiple tools to provide users with more awareness of the presence of connected devices [26, 36]. For instance, Huang et al. developed IoT inspector to identify all devices that are connected to the user's network and provide users with information such as device names, manufacturers, and IP addresses [26].

Researchers have also aimed to accommodate user's privacy needs through proposed privacy features and interfaces [19, 46]. Das et al. proposed personal privacy assistants to inform users about the data practices associated with the devices and configure the device settings according to users' preferences [19]. Yao et al. conducted a co-design study and identified several features such as data localization, and disconnection from the internet, that users desire in the smart home [44]. However, researchers found that end users are often unaware of the privacy controls already proactively provided by the device manufacturers. For instance, a recent study found that most end users are not aware of their ability to view and delete audio logs, even though those same users were not comfortable with the permanent retention of their recordings [31], demonstrating that such a privacy paradox may be caused by lack of awareness of available features. Moreover, some of the privacy controls are misaligned with users' needs. For instance, Google Home and Amazon Echo offer a physical mute button that requires different interactions than regular voice commands, and hence the button is rarely used [29]. Nevertheless, smart home users' decisions about the device features and controls were driven primarily by

functionality and convenience than privacy [21]. Several studies have looked more specifically at the access control mechanisms in the smart home [25, 40, 41, 46], examining the design needs and uses for people sharing devices with others. In a large scale vignette study, He et al. found that users have complex preferences that depend on multiple contextual parameters at once, such as time, location of the device, and people [25]. Tabassum et al. suggested providing more granular access control mechanisms to share the device with non-household members [40]. Users tend to opt for a more intrusive approach, such as account sharing, rather than permission delegation when the privacy controls do not match their needs [16]. Zeng et al. developed a prototype interface which included location-based access controls, supervisory access controls, the ability to ask for permission (i.e., reactive access control), along with notifications on how other users are using a device. However, in a field study, they found little use of nuanced access controls either because of the complexity of setting up the policy or the strong trust among the household members [46].

Considering these challenges, several studies have examined the design space for smart home privacy mechanisms and controls. Mare et al. evaluated seven smart hubs on their design choices around access control, privacy, and automation and found tensions between different stakeholder values such as privacy, security, usability, and reliability [32]. Furthermore, Feng et al., introduced a design space taxonomy for privacy choices in IoT [22]. They present five key dimensions: choice type, functionality, timing, channel, and modality to consider for providing meaningful privacy controls.

These works provide a valuable basis for future privacy design in the smart home. Yet, research on how end-users perceive and utilize the existing controls available for configuring, monitoring, and sharing smart home devices is still lacking. Hence, our work aims to understand the considerations users may have when configuring and managing their smart home devices, the associated privacy concerns, and how that affects the people's privacy surrounding these devices.

3 Methodology

To explore end users' perspectives of available controls in smart doorbells and locks, we conducted two sets of semi-structured interviews with novice users interacting with these devices for the first time, as well as current owners of these devices. Users are likely to spend the most time configuring and utilizing controls while initially setting up their devices. Thus, we sought participants who were not device owners, and invited them to go through the process of setting up two devices as though they were their own, so that we could observe this process. We also interviewed participants who do own these devices, and asked similar questions about how they currently use the device controls. We interviewed the owners of these devices to check whether the considerations from novice participants reflect practice, how that may evolve as the users get comfortable using the devices, and examine real-world considerations beyond the initial installation.

Both interviews centered on the awareness mechanisms and controls available in the smart doorbell and smart lock. Awareness mechanisms inform users of the data collection and sharing of the device. For instance, the event history informs users of the videos that are recorded by the doorbell and the access sharing interface helps users be aware who has access to the doorbell. Controls can be applied to manage what data is collected and shared and how to be notified of that data collection. In these two devices, these are controls related to notifications (i.e., turn on/off receiving notifications), data (i.e., download, share and delete specific data points), and access (i.e., share the device with multiple people). Table 1 summarizes device features, awareness mechanisms, and controls that were focused on in our study. The study was approved by our university Institutional Review Board (IRB).

3.1 Interview with novice participants

Participants who did not own the devices needed to come to our lab to interact with a smart doorbell and lock. Thus, we advertised for this study by distributing flyers in nearby neighborhoods, and on university mailing lists for faculty and staff. We sought people who were potentially interested in owning a smart doorbell or lock but did not currently have either of them.

Potential participants were asked to first fill out a pre-screening survey regarding the types of smart home devices they have in their house. We recruited participants who were at least 18 years old, could come to the lab to participate in the study and did not own a smart doorbell or lock. However, they may own other smart home devices.

We recruited 21 novice participants (N1-N21). Twelve of them were female and the others were male. Five of the participants were computing professionals. Participants were in different age ranges: 3 participants were 21-30 years old, 8 participants were 31-40 years old, 2 participants were 41-50 years old, 6 were 51-60 years old, and 2 participants were 61-70 years old. We refer to these non-owner participants as novices for the remainder of the paper.

We invited these participants to our lab for the observation and interview. The interview was audio and video recorded, and lasted on average 50 minutes. Participants were compensated with a $15 Amazon gift card for their time. The interviews were conducted October and November of 2019.

As a part of the interview, the participants interacted with a smart lock (Nest Yale lock) and a smart doorbell (Ring doorbell), using the device's app installed on a lab mobile phone. The interaction was necessary as we wanted to understand how new users perceive and want to use the controls provided in these devices. For each of the devices, we asked participants to go through and configure different features related to notification, data, and access control as they would if they were configuring the device for their home. Participants were asked to think aloud as they were exploring different features of these devices. After exploring each feature, we asked participants several follow-up questions on their perceptions, how they envision their use, and any additional information or controls they expect for that particular feature. For example, after participants explored the device sharing interface, we asked them with whom they would want to share the device with, what access they would want to share, what they think about the current interface controls, and how they would change them to better satisfy their anticipated needs. Finally, we collected participants' demographics at the end of the interviews. The complete interview guide is provided in the Appendix A.

Device	Features	Awareness mechanisms	Controls
Ring Doorbell	Motion detection	Notification, event history of recent activity & recorded videos	Motion zone customization, enable/disable & scheduling notification
	Ring detection	Notification, event history	Enable/disable notification
	Video recording	Notification, event history	Download, delete & share video
	Access sharing	Notification, Access sharing interface	Add users with different roles, delete users
Nest yale lock	Lock/unlock detection	Notification, activity log	Enable/disable notification
	Auto-unlock (i.e., automatically unlocks door when users arrive home)	Notification	Enable/disable auto-unlock
	Auto-lock (i.e., automatically locks door after a set period of time)	Notification	Enable/disable auto-lock
	Access sharing	Notification, Access sharing interface	Add users with roles, delete users & add/remove temporary codes

Table 1: Summary of device features, awareness mechanisms and controls

ID	Gender	Doorbell and/or lock owned
D1	M	Ring doorbell
D2	F	Nest doorbell
D3	M	Ring doorbell
D4	F	Ring doorbell
D5	M	Ring doorbell
D6	F	Ring doorbell
D7	M	Ring doorbell
D8	M	Ring doorbell
L1	M	Schlage sense & August lock
L2	M	August lock
L3	M	August lock
L4	F	Kwikset lock
L5	F	Kwikset lock
L6	M	Schlage connect Z-wave plus lock
DL1	M	Ring doorbell & Kwikset lock
DL2	F	Ring doorbell & August lock
DL3	M	Ring doorbell & August lock
DL4	M	Ring doorbell & August lock

Table 2: Devices owned by owner participants

3.2 Interview with owners

We advertised this study by distributing flyers in nearby neighborhoods, as well as posting in smart home-related social media groups. Potential participants filled out a pre-screening survey regarding the devices they owned. We recruited 18 participants who owned either a smart doorbell (D1-D8) or a smart door lock (L1-L6), or both (DL1-DL4) and were using the device(s) for at least one month. Table 2 exhibits the devices owned by the owner participants. One participant was 18-20 years old, four participants were 21-30 years old, four participants were 31-40 years old, six participants were 41-50 years old, and three participants were 51-60 years old. Six of the participants were female and others were male. Seven of them were computing professionals. We did not specifically target people with a computing background, yet we believe the topic of the study likely attracted a high number of technically-knowledgeable individuals.

The interview with the existing smart doorbell and/or the lock users was conducted over the phone. The interview was audio-recorded via Google Voice. Immediately following the interview, the recording was downloaded and stored on our university infrastructure, and participants' phone numbers and the recordings were deleted from Google Voice. As most participants only discussed one device, and did not interact with their devices, interviews were much shorter than anticipated at 15 minutes on average. Participants were given a $10 Amazon gift card for participating. The interviews were conducted in November and December of 2019.

We started the interview by asking general questions about why they chose to buy that particular device and how they use it in their day-to-day lives. Participants were then discussed how they configured the smart doorbell and/or lock based on their needs. They were prompted to talk specifically about the controls they use regarding receiving notifications, logged events, and sharing the devices with others. We asked them how they are currently using those features, their concerns, and what other information and controls they would prefer to have in these devices. Participants' demographics were collected at the end of the interviews. The complete interview guide is available in the Appendix B.

3.3 Data analysis

We first used an inductive coding process to analyze the novice interviews. Two researchers independently coded the interviews of five participants and came up with a list of common codes. The research team then discussed and merged the codes and agreed on a shared codebook with nine structural codes divided into 34 sub-codes. The rest of the interviews were independently coded by the researchers using the codebook. After all the interviews were coded, the researchers met and discussed the codes. They discussed the disagreements and agreed on the code. There were a few instances where the coders could not resolve the disagreements. The whole research team met, discussed, and resolved those disagreements.

Once the coding was complete, the whole team met, examined the codes, and grouped them into initial themes. The themes were then discussed and adjusted in multiple group meetings. Our coding process involved multiple rounds of meetings, coding, discussing, synthesizing, and revising. Our coding process aimed to discover

the emerging themes as a research team, not seeking agreements on individual codes. The reporting of inter-coder reliability is often omitted in such qualitative coding [34]. Hence, we did not report the inter-coder reliability between the two coders who did the initial round of coding.

One of the researchers then used the same codebook from the study with novice participants to code five of the owner interviews. The codebook was then modified to reflect the structure of the owner interviews and discussed by all the authors. The final codebook for the owner interviews emerged with five structural codes divided into 15 sub-codes. The researcher used this codebook to code the rest of the owner interviews. Once the coding was completed for all the interviews, the codes were sorted and grouped into potential themes. The themes were used to write the narratives in this article.

4 Results

Overall, both sets of participants found most of the interface controls usable and understandable. As expected, many of the considerations driving users' decisions related to features of the devices rather than privacy. However, the decisions users made regarding device controls do have implications for what information would be collected, and how it would get used and shared. Thus, to report our results, we first discuss users' perceptions and privacy implications of the various sets of controls they interacted with or discussed, before presenting several additional themes that emerged from the study.

Our novice participants approached the devices with few expectations and learned about the possible features and controls through their interaction with the companion app. While we did not observe device owners interacting with their devices, participants were still able to discuss how they used the same features and settings. Thus for each subsection, we first describe the novice participants' perceptions and considerations, followed by the owners, and ending with a summary relating the two sets of results.

4.1 Notifications

Notifications are a key awareness mechanism for smart home devices, providing users with continuous knowledge as to what the device is capturing. For instance, the motion notification from the smart doorbell makes users aware of the device's ability to detect activity around the door and that a video is recorded as a part of that. Thus, one focus of our interviews was on the different types of controls that customize the delivery of notifications. While notifications are utilized by both smart doorbells and smart locks, participants sought to configure notifications more frequently with the doorbell because of the potentially higher frequency of unimportant notifications with that device.

For novice users, one way they sought to reduce notifications was to not trigger an event in the first place. All of the novice participants appreciated the ability to tweak the coverage in front of the smart doorbell to detect motion only in their desired area as part of reducing unwanted notifications. Sixteen of them further wanted the ability to turn off, pause/unpause and schedule the delivery of notifications. They described many different use cases for eliminating notifications, such as turning off motion notifications when there are known motions in front of the door, turning off notifications when at home or at a particular time of the day, pausing notifications for some time because they are busy or prefer some quiet time, etc.

Several novice participants sought even smarter notifications, such as wanting notifications only when a package delivery occurs or a person or something large or substantial sets off the motion sensor of the doorbell. Five novice participants also desired the doorbell to have the ability to identify the faces and voices of the people and surrounding sounds and notify them of unknown people and emergency events (e.g., break-ins, gunshots).

In contrast to the doorbell, most novice participants wanted to receive lock/unlock notifications from the lock all the time. However, five novice participants only wanted to receive such notifications when no one is home.

The owner participants discussed using similar notification controls for their doorbells. All of them tweaked the coverage area and motion sensitivity to reduce unnecessary motion notifications. Three owners discussed setting up people-only notifications, while two of them stated that they would like to receive notifications only when an unknown person triggers the motion. For example, D2 mentioned: *"I would like it to only notify me if it is a person not on a specific list so that I do not have to have it tell me when I am alone at the door."* Five doorbell owners noted that they pause notifications sometimes or schedule the delivery of motion notifications. For instance, DL4 mentioned:

"When we are home, it does not alert us if there is motion, it will only alert for the doorbell when we are home... I did not want cars passing by on the street to sensor it. And we have small kids who run in and out all the time, so I did not want every thirty or sixty seconds to say "motion at your front door."

However, none of our lock owners discussed turning off or scheduling the delivery of notifications from the lock. All participants preferred to receive the lock notification all the time, similar to the novice participants. However, while a few novice participants wanted to snooze lock notifications when they knew someone would be home, no owners implemented or desired this behavior.

For both sets of participants, the primary motivation for configuring notifications was to not be bothered by events that participants did not care about, primarily for the doorbell. Users' considerations of how they would customize the notifications may directly affect what is getting recorded and how it would be accessed and used. All participants desired to control the field of motion detection for the doorbell camera, for instance, impacting both data collection and notifications. However, in many cases participants configured or desired controls to customize the delivery of the notification, and still wanted the doorbell to record video when motion was triggered. Yet hiding notifications without turning off recording means that users will have reduced awareness of how often the doorbell is recording, leading to increased risk of recordings they would not want. For example, users may forget that the doorbell is recording a sensitive conversation near the front door because the motion notification was turned off.

In addition, the desire to be notified only of events of interest may actually increase the need for collecting certain types of information. For instance, participants may need to share their location

with the smart home device if they want to have different notifications when they are home or away, like DL4 above. Similarly, notifications of strangers would require facial recognition and the storage and identification of known people. However, users may remain unaware of how those identities could be used or shared for this desired feature.

In summary, participants' configuring the field of motion detection would potentially serve to limit data collection of a doorbell, while desires to use location-based features (i.e., scheduling notifications based on location or presence in the home), and recognition-based features (i.e., notification for only unknown person or voice) will increase the collection and use of users' data. Moreover, end users' awareness of such data collection and use may be reduced by their desire to disable notifications without turning off recording.

4.2 Storage

One of the common privacy issues with smart home devices is where and for how long collected information is stored, as users are often confused or unaware of these practices [39]. Many of our novice participants did not directly raise a concern about this issue from a privacy perspective. Rather, sixteen of the novice participants talked about the device's storage capacity while interacting with the activity log. They wanted to access the past history for a minimum number of days; however, they did not want the data to take much space in their phone's memory. These considerations led them to question whether the data would be stored locally or in the cloud and for how long. Not surprisingly, novice participants were more concerned about the storage capacity of the smart doorbell than the smart lock.

In fact, the novice participants were confused about how long the logs will be stored, as they could not find that out readily from the app interfaces. The study interviewers had to provide them with that information when asked. Interestingly, novice participants were not always happy about their limited capability of accessing collected information. For instance, when we mentioned that the Nest Yale lock shows only ten days of activity history, half of the novice participants (n=10) said they wanted to be able to go back further than that. N6 mentioned:

"As with the Nest thermostat, I can only go back a few days! I find it really annoying. I don't understand - we have the cloud. Why do we have to limit this? They are still holding onto our data, almost guaranteed forever, so why not show that to us? And again, it's a couple of bytes; it's not like there is a lot of information here."

Novice participants appreciated their ability to delete the data. However, most of them considered removing the data only for two reasons: limited storage (*" I don't know how much storage does it (doorbell) have. If it's going to your phone and I'm saving it, then that's taking up the storage on my phone as well. So like does it have an auto-delete function? Like I can set after 30 days, delete my videos."*, N3) and recordings of sensitive content (*"Let's say I go check the mail in my underwear. I might want to delete something like that."*, N6). Yet, novice participants seemed to have expectations that the device manufacturer was storing their data regardless, potentially indefinitely.

The majority of the doorbell owners had an online subscription to store their videos for a specific period of time and were comfortable with that. In contrast with the novice participants' expectations, owners reported rarely performing data deletion, with only two owner participants regularly deleting their recorded data as a privacy precaution. Two other owners wanted an easy option to *"just wipe out everything, you know, delete all my stored videos and any information like that, if I were to cancel my contract with them."*, D8. Similar to novice participants, owners also believed that deleting their information would be ineffectual as the company may retain the data. For instance, D4 mentioned: *"Well, regardless of what Ring says, there is no expectation. As far as I'm concerned, anything that is recorded it's at their discretion."* D4 was also concerned about unauthorized access to the data. He said: *"the problem is that they do keep your recordings, and there are people accessing them regardless of what they tell you....you don't know if there are third-party developers or applications or connectors that can be misused elsewhere."*

As such, some owners (n=5) expressed their desire to store the data from smart doorbells locally to limit sharing it with the manufacturers in the first place. DL4 mentioned: *"I am philosophically not exactly happy that I am sending all of my data to the Google cloud and that now Google can recognize certain people."* Depending on the device, there are methods for maintaining a local server. However, the complexity of performing this setup and configuration discouraged the owners from doing so, even though it could give them more control over their data. No owners reported attempting this except L6, who installed an encrypted drive in his basement to store data. While discussing the configuration, he mentioned : "I physically installed the lock, I went and grabbed the pairing number and punched it into the universal device controller immediately, and that allowed me to go into the controller and program all of the codes and set-up a log function so that it emails me when ever it is actuated. I have an Ajax web interface allowing me to turn things on or off. I had to go purchase a third-party app so that I could have an app on my phone. The console is a windows 2000 console java app that runs on a computer." He is an IT professional and was comfortable with this complexity of setting up the lock.

Overall, our novice participants expressed little interest in proactively removing their data when storage is not a concern, and owners seldom erased data on their own. Both sets of participants desired to keep a long-term history, even longer than some devices offer. However, both owner and novice participants mentioned that much of the recorded data was irrelevant or trivial and not actually needed, such as *"packages left after you make sure you got them."*, N13. One of the implications of participants' lack of interest in removing data is that organizations would have an immense amount of information to use for additional inferences, for example. Yet, many participants already expected this was occurring anyway, regardless of their settings. Despite their discomfort over such additional uses, they did not expect to be able to control that and appeared resigned to it occurring. This gave them little incentive to delete data proactively.

4.3 Video recording

Past research has shown that video and audio are considered as some of the most sensitive data collected by smart home devices [13, 37]. In our study, this only involved the smart doorbell.

Most of our novice participants were comfortable with the audio and video recording capability of the doorbell since the device only records outside of the house. However, eight novice participants shared their concerns about the doorbell recording sensitive video/audio or picking up audio from inside the house. Some novice participants (n=7) talked about their desire to actively turn off the recording for some time (e.g., when kids are playing in the yard) to reduce their concerns. For instance, N7 mentioned: *"does it (doorbell) have an on/off button if you want to turn it (recording) off? (I want to) be able to do that with my phone."*

Several of our novice participants also discussed the doorbell's ability to record bystanders. Four of them did not show any concern about that. These participants mentioned that what the doorbell is recording is already public and could be helpful in some cases for the neighbor if the device catches suspicious activities on their property. N11 adamantly stated: *"Because it would be at my house and so it's my stuff. Maybe the people that were there might not necessarily be comfortable, but it's how the technology works, so get over it, people."*

However, three other novice participants mentioned their concern about being recorded by others' doorbells: *"People can be pretty weird about their lawns... So, what if I am going up to someone's house and they aren't there and I am going to drop something off real fast? and then they watch it and they're like oh my gosh... I can't believe she walked on our lawn." (N5).* These participants discussed taking measures to reduce recording bystanders. N5 mentioned she would want to stop recording while having an event in her house. She said: *"I would probably be more self-conscious (if recorded by others), and they probably would be more self-conscious for coming into our house too. I'm not sure how welcome people would feel. If they think I can see all of this stuff and that I could, then they might not feel so welcome."* Furthermore, N2 and N6 wanted to configure the recording range of the video doorbell: *"I'm not sure whether this (doorbell) has the ability even to do a field of view to define a certain width."* However, one thing to note is that the field of view (the area that gets video recorded) is different than the motion sensor coverage area (the area that senses motion). Thus, bystanders may still be recorded, even when they do not trigger the recording. However, turning off the recording or limiting the field of view may lead to missing unexpected but important information and thus influence users to instead just restrict notifications and not the recording itself.

Though some of our owners were concerned about the recording capability of the smart doorbell, they became comfortable using the device with the practices they adopted to reduce undesired data collection. These practices included not having a private conversation in front of the device, using only live view features so that videos do not get recorded, or knowing they could delete if a sensitive video gets recorded. Even so, three of the owner participants experienced an event where the smart doorbell recorded unexpected audio or video of either their family members or bystanders. For instance, D2 mentioned:

"People do not really recognize that you can listen in on conversations or watch them. When my mom was visiting me, they have the camera set up in San Francisco, and her in-laws were visiting. So my mom would sit there, and she could listen in on my grandmother gossiping about her to the other relatives, and my grandmother had no idea that she was being recorded. I don't want others to have that ability to watch me 24/7."

D2 shared his experience of how their doorbell had recorded his neighbor: *"I found out my neighbors purchase of truck because he was just chatting on the phone outside in his backyard. My video doorbell camera picked up on his voice, and he was talking about loans and stuff. But he did not give me consent to listen in on that conversation, but I could just because I put it on my property."*. Although some were concerned, no one took any actions to limit recording bystanders. Prior studies found similar concerns about sensitive audio/video getting recorded for smart speakers [29] and indoor security cameras [39].

In summary, the novice participants showed more concern and desire to take action to limit the recording of themselves and bystanders than the owner participants reported doing. The owners were comfortable with the current recording set-up of their doorbell, despite several having stories of undesired recording. Though a few owners were concerned about recording bystanders, they were unsure about how bystanders' privacy could be better respected. Thus, the implications for users is that permitting the video doorbell to record even when it is not necessarily desired increases manufacturers', and potentially other stakeholders', access to the users' data. Data collection by such a device could be reduced by limiting the field of view of the recording, disabling the video and/or audio recording when not necessary and behavioral restraint around the doorbell.

4.4 Video sharing

One of the main reasons for using smart doorbells is to ensure the safety of the household. Participants desired to do so by sharing any suspicious videos (e.g., someone stealing packages, house or car break-ins, or randomly roaming around the house) captured by the doorbell with their family and the police.

Several of our novice participants (n=9) wanted to promote the safety of their neighborhood by sharing any suspicious videos with neighbors and neighborhood communities (e.g., Nextdoor, Ring Neighborhood). Moreover, six novice participants mentioned they would also share anything they deemed funny. For instance, N6 mentioned: *"(I would share) if something funny, you know, if like the mailman was carrying a package and he slipped on the front doorstep."* Thus, bystanders could be completely at the mercy of the doorbell owner whether or not compromising video of them would go public.

However, some novice participants showed concern about sharing videos on a public platform. N5 decided she would not share the videos on any public platform. She said: *"Once you post it you don't have control over it. I would just reach out to individual people. Our specific neighborhood has a closed network. But that closed network would exist on social media, and anyone could take any of that stuff and start a new chain and distribute it."*

She was also concerned about others sharing videos and what information could be inferred from that. For instance, she mentioned: *"If my kid walked up near anyone's door, then they could share that on social media, and I wouldn't know what kind of location information is in it. If there is location information in it, can they tell where they (kids) are?"*. Two novice participants mentioned that

they would prefer to share a snapshot instead of the whole video and wanted an easy option to do that from the app. N17 thought about ownership while talking about sharing video: *"To what extent that video is shared, and the rights to that video say, uh, if they can be subpoenaed for Police use or something like that. I don't know exactly the privacy rights of that information, whether or not Amazon owns it, or I own the videos."*

Our owner participants also said they would share the videos with neighbors and the law enforcement if it is related to their or others' safety. Some of these participants mentioned looking through the community apps such as Ring neighborhood to keep updated about their area. However, none of them reported sharing any videos on these apps. In fact, D6 and D7 showed concern with sharing videos using the Ring app's 'neighbor' feature. D7 mentioned: *"I would like to ensure that community is very secure and there's no way that any of personal information (other than the video) could possibly be shared through the neighbor feature without my knowledge."* D6 shared his preference to download the video and share it via personal message or email.

Ultimately, sharing a video on a public platform results in ubiquitous access to the video. Such access can be limited by sharing only a snapshot rather than the entire video or sharing through a personal channel when possible. Both owners and novices expressed their willingness to share suspicious videos and random funny videos with their family, friends, police, neighbors, and social media. However, most of the owners did not experience any event where they felt the necessity to share it with others. Yet, our participants had concerns over the ownership and control of those videos, which were not alleviated by the interface.

4.5 Activity and access monitoring

One of the primary goals of having smart home devices is to monitor the activity with or surrounding the devices via notifications and the activity logs available in the app interface. Many of our novice participants (n=12) discussed utilizing these features to monitor bystanders of these devices, especially less trusted people such as house sitters, Airbnb guests, etc. For instance, N17 mentioned:

"Because sometimes when we were out, we'll have somebody like feeding the dog, so I don't want this kid coming to the house and invite an old girlfriend over... I want to know when he's in there, what kind of activities going on."

A few other novice participants also mentioned they would use the smart lock (n=2) and smart doorbell (n=2) for parental monitoring. For instance, N16 mentioned: *"My wife loves to know when my son is coming in the house. He's 19. He got a girlfriend, you know, he can come in at 1:00 or 2:00 in the morning. He's got rules, don't get me wrong, if he decides to come in late, you know, he could be flagged. We would want to know that, like when he rolled in the house... It's a nice way (through the smart lock notification and activity log) to monitor my kids if they decide to sneak out in the middle of the night, sometimes."* Prior studies have also identified the potential tension between parents and teens, especially with monitoring via entryway cameras and locks [42].

In addition to monitoring activity, many novice users also wanted to monitor possible unauthorized access, especially for the smart lock. Almost half (n=10) of them wanted notification from the lock when someone attempts to disengage the lock, tries to open the door with an invalid code, or attempts to use their code outside of particular schedule. For instance, N9 mentioned: *"(I want a notification) if someone tries to pull it off the wall to disconnect it, if someone tries to tamper with it or bash it, there should be sensors for that."*

Similar to novice participants, owners also appreciated the notifications from smart doorbells and smart locks in monitoring the safety of their house and the residents. For instance, DL4 mentioned: *"If my daughter texts me and tells me that she's walking home from school, then I'll wait for that August notification telling me that she opened the door so I know that she made it home OK."* However, owners did not discuss any use cases for the activity logs of the smart doorbell or smart lock.

Thus, notifications were the primary means for participants to know about the activities around their devices. Though the novice participants appreciated the idea of having the activity log, the owners seldom used it, especially for the smart lock. Both owners and novice participants wanted to look at what they are particularly concerned about (e.g., whether and when kids got home) or when something goes wrong (e.g., someone entered the wrong passcode, error in locking the door). Here again participants expressed desires for smarter notification mechanisms, or for more advanced log filtering mechanisms based on the person, time, or errors, to help them with their particular needs.

4.6 Access control

Our participants wanted to share their devices with others, both within and beyond the home, and smart home devices provide various capabilities to enable this sharing. For example, For example, the Ring doorbell allows owners to add an unlimited number of shared users to the device [7], while the Nest Yale lock provides options to add users as a guest or an owner or share only a temporary entry code without access to the app [8]. Our novice participants discussed they would share full access to their doorbell and lock with other trusted and older house residents, e.g., spouses, older children, etc. Similar to prior work [40], they also acknowledged the need for sharing the device and continuous access with less trusted people when they go on vacation or in case of an emergency. However, most of these novice participants did not want to add such users as shared users, especially for smart locks. Instead, they wanted to provide them access via sharing codes to access the lock.

In the case of adding non-trusted people to the app, novice participants wanted to understand what capabilities and data were being shared in these instances. Specifically for the smart doorbell, they wanted to make sure that the shared users do not have access to the device settings and past logs and only have access to the events (i.e., video recordings) from the point in time when the device is shared. For instance, N16 wanted to share his doorbell with his neighbor and said: *"They wouldn't have access to past (recordings), right? So do you get anything historical? If I'd hired a lady escort... So essentially, they could see it up there and say, what's she doing up his door?"*.

Thus, the device sharing interfaces of the Ring doorbell and Nest Yale lock led to concerns among novice participants, as the interface does not provide any specific information on what capabilities and information are being shared with another user. For instance, while

interacting with the Nest Yale lock's access control interface, N8 frustratingly said: *"Don't know the difference between add a guest and add a home member."*. The interface's vagueness also led some novice participants (n=8) to believe the shared users would have the same access as the device owner.

Three of our novice participants also emphasized the importance of authentication for controlling access. N4 said his kids sometimes use his phone and was concerned that they could get into the app and change the lock settings. N6 had similar concerns with his kids activating the privacy mode button in the Nest Yale lock without proper authentication. He said: *"Because I do have children, they would just go touch that button (the privacy mode button), and I just go outside without my phone and think I can just use the keypad, and now I'm locked out of the house. So, it is definitely a concerning feature that could work against you very easily."* N12 wanted to set a password to control access to the recorded video on the doorbell.

Beyond just the sharing capabilities, two novice participants also expressed the need for feedback mechanisms from the devices when shared with other users. They wanted notification when the shared users accept/decline the invitation. They also wanted to know what processes the shared users have to go through to accept the invitation so that they can help, especially when the shared user is non-tech savvy. For instance, N18 mentioned: *"If I was sending it (lock passcode), and I'd be more familiar with it. I might have put a couple of comments in there like what they have to do: something to kind of light it up first, you know, like tap it or something, then you hit the button, it makes a noise and says hey, what's the code? Because that could be a little bit confusing to someone, to know just initially how to activate it."*

Our owner participants shared their doorbell only with close and trusted people. For the smart lock, they opted for remotely opening the lock for a visitor or sharing codes to access the lock. Some shared their preference for such non-app access for doorbells as well, such as sharing a one-time link to view a live stream. However, they also recognized that a shared link or temporary code could be shared with someone else without the owner's knowledge. D4 mentioned: *"I would not want to send a link that anybody could open; I would prefer it forces you to register somehow so that I can revoke access at any time. It's not just giving off a link."*

Owners wanted an easy and fast way to share their devices with trusted people, but the interface did not necessarily meet their needs. For instance, three owners shared the device with their family members by sharing the full account credentials because they found it more convenient than using the sharing interfaces of their devices. Another owner, L3, shared access with his spouse through a smart speaker instead of sharing the app, and controlled access from others through available authentication features. He integrated his August lock with Amazon Alexa and used an authentication code when operating the lock from the smart speaker. He said: *"You can tell it (Alexa) to unlock, but you have to have a certain code... It will ask you for the code, and when you get the right code, only then it will actually unlock the door."* Similar to novice participants, owners also discussed the need for more granular access control features while sharing with non-trusted people [25], and as such, did not report sharing the access to the app with others outside of close family members or roommates other than sharing temporary codes for locks.

The lack of transparency and control limited users' willingness to share their devices. Both owner and novice participants were comfortable sharing their devices only with close and very trusted people using available methods. However, confirming the findings in prior work [25, 40], our participants were concerned about sharing access with less trusted people (e.g., kids/teenagers, visitors, neighbors, house-sitters, etc.) and wanted transparent and granular access control features. Beyond confirming findings from prior research, our results provide new details pertaining to the need to control access to past logs, provide one-time access, and provide additional feedback mechanisms for non-tech savvy and/or less trusted shared users.

In summary, participants' practice of sharing account credentials to share their devices increases access to features and data collected by the devices. However, participants were comfortable with this because they only showed this behavior when sharing access with very trusted people. In contrast, sharing one-time, temporary, and capability-based access reduces non-trusted users' interactions with the device. One novel finding of our study is that users need transparency and control to not only restrict shared users' access to specific capabilities [25, 40] but also to block them from accessing and downloading particular data points already stored in the device.

4.7 Emerging themes

Several additional themes emerged across the range of controls and features of the devices.

Building understanding: A common theme that emerged, particularly as novice users explored the controls, was the need for feedback and transparency mechanisms that would contribute to users' mental models of how various features work and their performance. For example, they appreciated the remote control and monitoring capabilities of the smart doorbell and lock. However, a few novice participants (n=5) felt uneasy about the lock and whether they could trust different features. For instance, N10 discussed his concern about using the auto-lock feature: *"I would think it would be somewhat dependent on how accurate your location tracking is. Like, I would be nervous about, did it work? Did it go on?"* These participants wanted notification from the device to make sure the device worked as intended, mostly when the device is set to perform some action automatically (i.e., auto-lock, auto-unlock).

However, the use of feedback mechanisms may change with time as the user gets comfortable using the device. For instance, N6 mentioned: *"I would be paranoid for a little while (with auto-lock) and probably check to make sure it did it, but after I got comfortable with it, I would trust it to do what it is supposed to do."*

Novice participants also exhibited concern about using a particular feature when they did not understand how it worked. For instance, the Nest Yale lock provides users with an option to get a notification when the door is unlocked after the last person leaves home. A significant number of our novice participants (n=19) were confused about how the 'remind me' feature works. For instance, N14 mentioned: *"I'm confused about how does that technically work? How would it know that my phone crossed the threshold of the front*

door? Like if it would just explain, whether it uses the GPS or something? That makes me nervous about it, but only because I don't know how it works."

Furthermore, N11 was concerned about whether this feature would require tracking of her location and who would have access to the location data. Please note that the app forwards users to their support website if they want to learn more about how the feature works, which provides detailed information on the feature. However, our novice participants were instantly turned off by the long documentation on the website. As N18 said: *"There's too much... too many words. This is a lot more to read than I want."*

As another example, novice participants were concerned about the device sharing interface when it doesn't provide specific information on the shared users' capabilities. The Nest app only allows users to set up home entry keycodes and asks users to install the Google home app to provide other types of access, which made the process more confusing for our novice participants. Again, Ring and Google offer detailed information on their support website. However, the issue is that this information is not explicitly provided in the app where the user is acting on the feature and has to purposefully search and read documentation to be informed.

One of our owner participants, DL3, in fact, mentioned that the August lock interface is more informative, as it shows capabilities available to different access levels and is more user friendly. Therefore he decided to share the lock using the app sharing features, whereas, for the Ring doorbell, he directly shares his account credentials with his family members. In general though, owners did not discuss the need for feedback and transparency nearly as much as the novices did. One reason could be the fact that they have already built up an understanding of different features through use and become comfortable using the devices. Or, they chose not to utilize features they were unsure of, and did not remember them enough to discuss them in the interview.

To summarize, feedback and transparency are critical for making novice users aware of how smart devices work and making them comfortable in utilizing the features. Many of the questions novice users had related to information collection and usage, such as how the door lock knew the users' location. Increasing the transparency and awareness of these features may increase the trust in the device. However, once a user becomes comfortable and no longer wants the feedback, such as our owner participants, that may reduce their awareness of data collection, leading to undesired privacy risks.

Trust as a prerequisite of purchase: Similar to previous research [47], we have also found trust as an important factor in participants' purchasing decisions. Four owners specifically bought their devices from companies they already trusted and have information available on the Internet about how they deal with the device's security and privacy. For instance, D5 owns a Ring doorbell and said: *"I think being backed by Amazon was really important to me because I wanted something backed by a company that was not just going to go away tomorrow... I knew that Amazon had made other range of security systems and stuff like that, and it just felt like there were going to be updates and stability around the whole system."*

Though owner participants put trust in the company that they will follow good security practices, it is not always clear how they define these practices (i.e., is it updatability, encryption, anonymization?) and what guidelines are available for consumers to support that determination.

Accepting defaults: We found that both owner and novice participants seldom changed the default settings, and only modified specific features to better serve some functional needs (e.g., customizing motion detection based on the position of the house, setting of schedule for receiving notification, turning on/off auto-lock and auto-unlock feature).

While users accepting default settings is common, we observed interesting reasons for this in our interviews. Three novice participants expressed a lack of confidence in their configuration skills and trusted the default settings for better performance from the device. For instance, N14 mentioned: *"I wouldn't want to customize this, because I wouldn't want to mess up the security of the automation of it. Right? I mean, I feel like whatever pre-selected settings are. I mean, they're probably pretty good for security."* One owner participant also mentioned a similar reason for not changing the default settings. However, most of the owners did not feel the need to review and modify the default setting unless it did not meet their functional needs.

Concerns about security: Similar to previous research, we found that participants are concerned about someone hacking their smart devices [39, 45] to intrude upon their homes or information. Sixteen novice participants showed concern about the smart lock, as the device provides physical access to the home. The biggest concern was that somebody might be able to hack the lock and would be able to know the lock status or unlock the device. For instance, N10 mentioned: *"You see in so many movies where they just plug-in a baby device and then all of a sudden, it's like "this is the code," and I'm like is that real? I don't know. So yes, security-wise, I would want to know my home is safe and not hackable."* The novice participants did not discuss any particular action they preferred to take other than locking down the lock keypad and relying on the company for the proper security of the lock. Five novice participants also mentioned they are concerned about the doorbell being hacked as with any of their Internet-connected devices.

Only three owners' shared concerns about the smart lock and changed their behavior to mitigate their concerns. DL1, whose main concern was: *"if the door's unlocked, it says it's unlocked, so someone was to get a hold of my devices they will know which doors are unlocked at any given time"*, mentioned regularly deleting the lock log and preferred to have an automated system to *"delete at midnight"* every day. On the other hand, DL3 mentioned adjusting the physical location of the lock: *"I don't feel that the smart lock itself is ready for the main door because I'm a little bit worried about someone hacking my system to my lock. That is why I didn't put it in my main door. Instead to the door connecting my garage to my house."* L6, an IT professional, bought a specific lock with Z-Wave plus technology and created a custom controller so the lock is not connected to the internet and can't be remotely attacked by an adversary.

Three other owners with locks discussed the possibility of hacking but were not concerned. L5 mentioned having a locked Wi-fi where DL2 and L1 believed: *"I feel like if someone is going to try to*

get into my apartment, they are not going to go through the hassle of going through my August account, they would just pick the lock or break down the door." (L1)

Owner participants were not as concerned about someone hacking the doorbell as the lock since it did not involve direct access into the house. Though owners of the doorbell did not specifically mention hacking, four of them did discuss security measures for protecting it, including using a secure password (D7, D8, DL2), or two-factor authentication (D4).

In summary, our participants were more concerned about the security of the lock than the doorbell. Novice participants showed more concern than the owner participants. However, participants primarily rely on the manufacturer for security, and only a few discuss taking diligent action to enhance the security of their devices.

5 Discussion

Device owners in our study reported configuring their devices and adjusting settings during initial installation. Our novice participants approached this process with few privacy expectations and desires, and instead learned about the device capabilities as they explored the interface. Participants were driven primarily by functional considerations, to achieve their goals for controlling or monitoring their homes. Previous research has similar findings indicating that functionality and convenience are the key considerations in the smart home [46, 47]. Yet those considerations have implications for how information about them and their homes is captured, stored, used, and shared, and how much awareness they have of those data practices to inform their decisions. One of the novel contributions of our work is that it highlights the privacy implications of smart home users' functional goals, particularly where those decisions could lead to additional data collection and extended data storage.

Table 3 summarizes the behaviors seen in our results. Some decisions or desires would serve to increase the collection of, or access to, information, potentially increasing the privacy risks. Several of these, such as using location information or filtering data logs, would increase the utility of their devices by reducing unwanted notifications or information. Thus, an implication for designers should be to ensure that users are able to make that privacy/benefit trade-off in an informed way. Other behaviors, such as not deleting information or sharing full account credentials, are utilized because the existing methods for deleting and sharing are still too burdensome and thus a target for improved designs in order to improve both usability and privacy management.

Other behaviors serve to reduce data collection and use, while at the same time serving users' functional or privacy needs. A few of these behaviors were commonly done, such as adjusting the motion detection zones of the smart doorbell to only trigger when desired. However, several other behaviors were rare even while other participants expressed interest in them, such as temporarily turning off video recording or locally storing information. Improving the usability of these capabilities would provide users with additional privacy-preserving controls.

Another important feature of smart devices is the ability to monitor one's home through awareness mechanisms, primarily notifications. These notifications serve an important privacy function as well, keeping users aware of the data that is collected by their devices and providing easy access to it. However, reducing unwanted notifications may also reduce that awareness, and again result in privacy risks if sensitive information is unknowingly collected or shared. The ability to monitor the environment also poses challenging privacy issues for bystanders, who have limited ability to control or monitor what is collected about them. Device owners are provided little guidance as to how to try and respect bystander privacy, despite some interested to do so.

The perceived benefit and cost impacted our participants' considerations and decisions on how they configure their devices. For instance, participants were willing to record videos even when they did not want notification for those events. Even though this behavior resulted in the manufacturing company getting access to more data, participants wanted the benefit of the recordings just in case something important gets recorded. The effects of perceived benefit and cost on participants' considerations are consistent with the privacy calculus theory [18]. Our participants tended to consider perceived benefits from the features more than the potential cost of losing privacy due to data capture and disclosure. Thus, the convenience outweighs participants' perceptions of low risk of privacy issues, and they do not take many actions to exercise the controls to reduce data disclosure, potentially heightening the privacy paradox [38].

Design implications and opportunities

The conundrum of default settings: From our interaction with the participants, we believe that many users are unlikely to review a device's privacy settings unless it is a part of the device installation process or they are explicitly nudged to do so. Most of the participants may continue using the device with the default settings, even when reviewed, due to their lack of confidence in modifying them. However, smart home providers do not always turn off privacy-invasive features by default. For instance, in Amazon Alexa, a portion of the voice recording is allowed to be manually reviewed by contractors by default; users must choose to opt-out [6].

Moreover, accepting default settings without reviewing them may further decrease end-users' awareness of the data practices. Users may not deliberately make privacy decisions if they encounter a predefined default setting decided by the manufacturers, minimizing users' opportunities to consider their privacy alongside their desired features and behaviors. However, manufacturers' primary concern is ease of use when installing a new product, which can benefit from making the configuration process as brief as possible. For example, Amazon is working on a zero-touch setup for Amazon wi-fi devices, such as smart plugs. With this setup, users would only need to plug in the device, and Alexa will automatically find the device and get it to work without the need for any additional configurations [2].

Yet, providing default settings is important as bombarding users with too many settings upon installation may result in decision fatigue. One suggestion is to prioritize those settings with the most implications for users' privacy, based on user research and input from privacy experts.

Increase data collection, access and use	Decrease data collection, access and use
Features based on face recognition	Store data locally
Features based on location	Auto-deletion of recorded data
Not removing stored videos	Turn off motion detection and audio and/or video recording
Sharing video recordings with others (i.e., police, social media, etc.)	Configure motion zones
Accepting privacy neglecting defaults without reviewing	Reducing camera's field of view
Filtering mechanism in the activity log	Behavioral restraint (i.e., limit conversation in front of the device)
Sharing account credentials to provide access	Share limited device/information access (i.e., a one-time link to see the live view)
	Only share particular capabilities with shared users (i.e., block access to device settings)

Table 3: Behaviors and decisions that increase or decrease data collection, access and use

In app information availability: Our study indicates the importance of providing explanations of features inside the app, alongside the controls. Users may have a flawed understanding of how a setting works if it lacks proper explanations. For instance, some of our participants thought shared users would have the same level of access as the owner since the access sharing interface did not readily provide that information. This lack of understanding may even lead users to avoid the feature and find a workaround that may have its own privacy risks. For instance, Tabassum et al. found that some smart home users share full account credentials to provide access [40]. Another more problematic behavior that users may exhibit is using the feature with incomplete understanding and getting comfortable with that. It may reduce users' awareness of the collected data and lead to loss of trust upon violation of their data collection expectations.

The current practice of smart home device vendors is to provide explanations of the features and controls in their websites. We observed that users are not good with such decoupled interactions. So in these cases, the most straightforward solution would be providing an explanation right in the place where it is most expected. However, one of the challenges is to present that information concisely in the small app interface. Too many settings on one page with lengthy explanations may overburden users and discourage them from utilizing the available controls.

Another suggestion is to provide a 'help and support' feature inside the app, where people can search for a particular setting, how it works, and its privacy implications. However, the challenge again is to present the information concisely and interactively. One possibility is to create short and interactive videos explaining the features. Future research needs to investigate how to strike the right balance of sufficient yet concise information.

Greater control over data collection: In our study, the controls for configuring notifications were often more sophisticated than the controls for limiting or pausing data collection. For example, while many novice participants mentioned wanting to turn off doorbell video recording for certain events, none of the doorbell owners reporting doing this behavior. We surmise that one reason is that pausing the recording was too much effort in practice [18].

Similar challenges for limiting data collection have been found in other domains. For example, Privolta, a company that specializes in privacy-focused ads, found that it takes 17 clicks to opt out of Google's data collection in the United Kingdom, while it only took one click to give the tech giant consent to collect one's data [3].

Thus, devices still need more nuanced controls to configure data collection. This includes having many of the same options as were discussed by participants for limiting notifications, such as being able to limit recording to certain times or certain kinds of events; temporarily turning off recording with automated restart; and only recording when the user is not at home.

An important aspect is to enable users to learn about the kinds of configurations that are possible, and keep them informed of the status of data collection to build their trust that controls are functioning as expected. One solution some devices have implemented are on-device physical buttons, such as a button to disable the camera, which can increase access to anyone near the device as well as trust that recording is actually disabled [4]. However, participants also raised a concern that the lack of access control over such features could have unintended consequences, and past research has found that similar features are rarely used [46].

Addressing bystander privacy: A challenging issue is how to provide controls for managing bystander privacy, and what options could even be made available? For instance, would options for a neighbor to negotiate their privacy with the doorbell owner, rather than talking to them in person, be useful? Also, what are the available resources for the owners to understand and be informed about the lawful collection and use of the videos that capture bystanders' audio or video? Smart home device designers should think about ways to better educate owners to respect bystanders' privacy. One way could be nudging users with available options when they configure their devices. For instance, as a part of the installation process, the doorbell can nudge users regarding whether their doorbell is capturing the neighbors' property and if they want to limit the field of view to block their doorbell from recording that area. Yao et al. [43] and Cobb et al. [17] have explored other easy mechanisms that could support bystander privacy, such as providing options to stop recording video and audio recording, to record only a specific area,

or to hide the face of bystanders when sharing video, and we believe our results further support the need for additional exploration.

The complexity of access control: Similar to the past research, our participants also wanted granular access controls and transparency over what accesses are being shared, especially when sharing with less trusted people [40]. However,our study extends the prior works by highlighting that not only do users need to block access to certain capabilities (i.e., deleting videos) but also to the historical data collected by the device (i.e., stored videos recorded before providing access). However, this requirement is not generally supported by the current devices. For instance, it is not clear from the Ring app or their support website whether or not shared users have access to the past recordings [7].

Another challenge is that while users state nuanced access control needs, providing for such detailed policies could lead to a very complex interface. This would likely lead to reduced usage, providing little benefit to users. Thus, research needs to examine the most common sharing scenarios with different devices and contexts, in order to provide sufficient, yet still simple, controls [15].

Another issue brought up by our participants is placing proper authentication mechanisms for controlling access, especially when the smart device is controlled by another device, i.e., a mobile phone, smart speaker, etc. For instance, an outdoor smart camera can be integrated with a smart speaker like Amazon Echo, such that it can be controlled through the companion app (the default interface) as well as through the voice assistant (an alternate interface). However, alternate interfaces can undermine a device's access control policy (set by the user) if the alternate interface cannot enforce access control. For instance, in the previous example, if the smart speaker cannot recognize the user issuing voice commands, anyone near the speaker can control the outdoor camera, irrespective of the access control policies set for the camera.

Privacy by design in the smart home

Privacy by design principles are one of the most recognized strategies for overcoming privacy issues by providing guidance on embedding privacy directly in the design of products [1]. The key goal of Privacy by Design is that privacy should be provided by default and proactively rather than resolving privacy infractions after they occur [15]. Our findings reflect several Privacy by Design principles, and provide additional guidance for how device manufacturers could incorporate privacy into their designs. Smart home device manufacturers can reduce privacy violations by providing privacy-preserving defaults for any settings that require direct end-user decisions during installation, such as whether the user wants to disable the doorbell from recording audio. Smart home apps should also nudge users towards other privacy-related settings on later interactions, to encourage users to consider controls even after initial installation.

Another principle that can encourage a more privacy-preserving smart home ecosystem is enhancing the transparency and visibility of the system to the end users [15]. This includes explaining manufacturers' data policies, how different features work, the data collected or shared to enable different features, as well as providing proper feedback on the users' input. However, the most challenging factor for smart home devices would be providing greater privacy without diminishing a device's functionality and usability, as these devices receive a vast amount of data and many features require access to sensitive information. Thus, designs should encourage awareness of what is occurring so that users can make informed trade-offs in order to meet their functional goals.

6 Limitations

We have conducted a laboratory study with novice users to observe their considerations as they install the devices for the first time. We understand that a similar in-person study with owners would provide in-depth details of the real-world consideration of users beyond the initial installation. However, we chose to conduct a remote phone interview to reach a broader user base. As a result, we do not have as detailed a view of their control interactions.

We also performed our study with novice participants using a Ring smart doorbell and Nest Yale Lock, as they are some of the most popular on the market. Hence, our participants' behaviors and decisions may be influenced by the app interfaces of these devices and their design choices, and not be generalizeable to other devices.

Many of our owner participants were recruited from the Ring doorbell user group from Facebook, biasing the brand of the doorbell owned by our sample. Moreover, almost all of our owner participants were the admin users responsible for installing and managing the smart home. Hence, our study does not provide the perspective of other household members, which may be different from the admin users. While our sample is fairly balanced in terms of gender and spanned a range of ages, our sample is skewed towards those over age 30, introducing bias in the data. Additionally, while we did not recruit within our own campus department, we did still attract a number of technical participants (almost one third of the study participants) who likely had deeper understanding of how smart devices operate. However, previous research found that more knowledgeable and less knowledgeable users in the IoT context still tended to implement the same security and privacy behaviors [39, 47].

7 Conclusion

Despite being driven by functional considerations, as our results demonstrate, privacy issues pervaded the decisions and concerns of our participants. These issues arose as participants contemplated data collection and storage, puzzled over how particular features worked, and sought to share their devices with others around them. Our results highlight a number of needs for improving the design of device interfaces to provide additional feedback and awareness to inform decisions and accommodate users' privacy considerations. Additional research will be needed to examine how improved control and awareness mechanisms could be designed while still keeping interfaces simple and usable. This research needs to also be extended beyond device owners who perform the initial installation and configuration, to the many other users within a home and beyond who may wish to have some control over the data collection and use of a smart device. Supporting the needs of the many different stakeholders of smart home devices, including bystanders, remains a major challenge that we will continue to examine as we further explore ways to support user privacy in the smart home.

Acknowledgments

We would like to thank our participants for their valuable time and input. We also want to thank the undergraduate and graduate researchers for their help with the recruitment and data collection. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] 2012. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers.* Retrieved 2022-09-10 from https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

[2] 2019. *Amazon wants smart home device setup to be a 'zero-touch' experience.* Retrieved 2022-09-07 from https://venturebeat.com/2019/07/05/amazon-wants-smart-home-device-setup-to-be-a-zero-touch-experience/

[3] 2019. *Default settings for privacy – we need to talk.* Retrieved 2022-09-07 from https://www.cnet.com/news/default-settings-for-privacy-we-need-to-talk/

[4] 2019. *How To Disable The Camera On An Echo Show.* Retrieved 2022-09-07 from https://bit.ly/3d6C1yV

[5] 2021. *3 ways to get consumers to trust internet-connected devices.* Retrieved 2022-09-10 from https://www.weforum.org/agenda/2021/12/3-ways-to-get-consumers-to-trust-internet-connected-devices/

[6] 2022. *Alexa for Business FAQs.* Retrieved 2022-09-10 from https://aws.amazon.com/alexaforbusiness/faqs/

[7] 2022. *Allowing Access to Shared Users and Controlling Ring Devices with Multiple Electronic Devices.* Retrieved 2022-09-10 from https://support.ring.com/hc/en-us/articles/211018223-Allowing-Access-to-Shared-Users-and-Controlling-Ring-Devices-with-Multiple-Electronic-Devices

[8] 2022. *Allowing Access to Shared Users and Controlling Ring Devices with Multiple Electronic DevicesHow to Invite Guests to Your Smart Lock.* Retrieved 2022-09-10 from https://bit.ly/3zBMHhH

[9] 2022. *Mozilla - *privacy not included.* Retrieved 2022-06-10 from https://foundation.mozilla.org/en/privacynotincluded/

[10] 2022. *Smart Tech in the American Home: Distrust or Trust?* Retrieved 2022-09-10 from https://www.mortgagecadence.com/blog/tech-in-the-home/

[11] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/soups2019/presentation/abdi

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

[13] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 1–23.

[14] Natã Miccael Barbosa, Joon S Park, Yaxing Yao, and Yang Wang. 2019. " What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes. *PoPETs* 2019, 4 (2019), 211–231.

[15] Ann Cavoukian. 2010. *Privacy by Design: The 7 Foundational Principles.* Revised: October 2010.

[16] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–16.

[17] 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.

[18] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10, 1 (jan 1999), 104–115.

[19] A. Das, M. Degeling, D. Smullen, and N. Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17, 3 (Jul 2018), 35–46.

[20] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.

[21] 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* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12.

[22] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–16.

[23] Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA, Article 268, 13 pages.

[24] 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)*.

[25] 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)*. 255–272.

[26] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13.

[27] Dongyeon Kim, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn. 2019. Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior* 92 (2019), 273–281.

[28] 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*. 1–14.

[29] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102 (Nov. 2018), 31 pages.

[30] Roxanne Leitão. 2019. Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. *Proceedings of the 2019 on Designing Interactive Systems Conference* (2019).

[31] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *PoPETs* 2019 (2019), 250–271.

[32] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications* (Santa Cruz, CA, USA) *(HotMobile '19)*. ACM, New York, NY, USA, 117–122.

[33] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart devices in Airbnbs: Considering privacy and security for both guests and hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 436–458.

[34] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 72 (nov 2019), 23 pages.

[35] 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*. 1–14.

[36] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. 2017. Iot sentinel: Automated device-type identification for security enforcement in iot. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2177–2184.

[37] 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)*. 399–412.

[38] Patricia Norberg, Dan Horne, and David Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *Journal of Consumer Affairs* 41 (03 2007), 100 – 126.

[39] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA.

[40] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. 2020. Smart Home Beyond the Home: A Case for Community-Based Access Control. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12.

[41] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*. HUPS 2014.

[42] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 129–139.
[43] Yaxing Yao, Justin Basdeo, Oriana Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3 (11 2019), 1–24.
[44] 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.
[45] 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
[46] 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)*. 159–176.
[47] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (Nov. 2018), 20 pages. https://doi.org/10.1145/3274469

A In-person interview guide: Novice participants

A.1 Arrival and Introduction:

"Hi, Thank you for taking the time to come in. My name is .... and I will be conducting the interview today. Please let me know if you have any questions throughout the interview process."

A.2 Consent:

The interviewer explained the consent form. Participants read and signed the in-person consent form. Participants received one copy of the consent form for their use.

A.3 Semi-structured interview:

"During the study, you will use a smart doorbell and smart lock."

A.3.1 ***Smart doorbell:*** " First I want to know about your expectations from the smart doorbell. Your answers will be audio recorded."

- How would you envision to use the smart doorbell in your day to day life?
- What kind of benefits do you expect to receive from having a smart doorbell?
- What type of concern would you have in using a smart doorbell in your house?

"Thank you so much. Here is a Ring Smart Doorbell. You can interact with the device using the app on this cell phone.

The camera and speaker will be on once you turn on the Ring doorbell. I'm going to walk in front of it a few times to trigger the motion. I'll also ring the doorbell so you can see what happens. If you would like you can test it and go in front of it, but if you prefer you do not have to be on the Ring camera at all. Any video that gets recorded now will be deleted off of the Ring device once we finish.

For the rest of this session, I'd like you to imagine that you are in your own home, and are using and configuring your device for the first time."

Event history settings (interface to view, share or delete recorded events): "Go ahead and explore this view for a few minutes and play with any of the features you would like to, as though it was your own device. Please think out loud, say what you are thinking, as you do so. "

- Which events do you think the doorbell stores?
- What information do you expect a video doorbell to show for each event?
- Is there any other information you would like to know about these events than what you saw in the app?
- What other events would you want the doorbell to store in history?
- What information would you want to be stored for that event?
- When do you think the doorbell records audio and video?
- Can you think of a scenario when you wouldn't be comfortable or wouldn't want the doorbell to record the audio or video?
- What kinds of controls for the event and video would you expect?
- What do you think would prompt you to download an event or video to your phone? Please explain.
- What do you think would prompt you to delete an event or video? Please explain.
- When do you think you would share an event with anyone? With whom would you share and why? Please explain
- Any additional controls you would want to have on the stored events?

Motion settings: "Now I want you to go configure the motion settings on the doorbell. Go to the Motion Settings tab, and configure this as though this doorbell was installed on your front door. Please think aloud as you view and modify the settings."

- What motions and activities do you think the doorbell will capture with the settings that you have?
- What concerns do you have about any of those events being captured?
- What do you think about the motion settings you have available to you?
- What other settings would you want to customize regarding motion?

Notification settings: "As you saw, this doorbell delivers notifications for various events."

- For which events would you expect to receive a notification from the doorbell?
- What information would you expect to pop up on the screen?
- When do you want to receive the notifications (ring and motion)?
- What do you think about the controls you have on setting up the alerts?
- What other controls would you want to customize receiving notifications?

Access control settings:

- Would you want to share the doorbell with anyone? With whom and why?
- What type of access would you want to give that person in your doorbell? Why?
- What features would you not want people to access? Why?

"Now go to the Sharing tab, and set up sharing for someone, using these fake credentials. Please think aloud as to what is going through your head while you are doing that."

- What do you think this person will be able to do with your doorbell?
- What features would you not want this person to access?
- What do you think of the device sharing interface and controls for this doorbell?
- What other information or controls would you want in terms of sharing the device with another person?

Follow-up questions:

- How did your concerns and expectations change after using the device?
- Are you satisfied with the features and controls available in the smart doorbell?
- Are there any other controls or features you want from the smart doorbell? What are those controls? How would you use those controls?
- How would you change the app to better satisfy your needs?

A.3.2 ***Smart lock:*** "First we will ask you some questions about your expectations from the smart lock. Your answers will be audio recorded."

- How would you envision to use the smart locks in your day to day life?
- What kind of benefits do you expect to receive from having a smart lock?
- What type of concern would you have in using a smart lock in your house?

"Thank you so much. Here is a Nest Yale smart lock. You can interact with the device using the app on this cell phone. Now we want you to use the august lock as you would if you have installed the device for the first time in your home. "

Notification settings: "First, go to the Notification setting and configure how you would want to receive notifications if this were your lock. Please think aloud as you do that."

- What kinds of notifications would you want to receive from the lock? For which specific events?
- When would you want to receive notifications?
- What information would you expect to pop up on the screen for each of these notifications?
- (look at the remind me feature) How do you think the Remind-me feature works?
- Are there any particular situations where the "Remind-me" feature would be useful? If so, what would they be?
- What additional features would you want to have regarding notifications?

Event History settings: "Now go to the History tab and examine and configure the event history."

- What events do you believe the lock may store?
- What information do you expect it to show for each event?
- Are there any other events that you would want it to store?
- What do you think would prompt you to delete an event? Why?
- What additional controls would you want to have regarding the lock's events?

Access control settings: "Please configure the lock to share it with someone else – you can use these fake credentials."

- Would you want to share access to the lock with anyone? With whom and why?
- How would you use the family and guests roles in sharing access to your lock?
- How do you feel about the family and guests interface and controls in general?
- What additional controls would you want that are not offered in order to share access to the lock?

Nest Yale lock specific features:

- What would you expect the "privacy mode" feature to do?
- When do you think you would use this feature?
- Do you have any concerns about privacy mode?
- How do you think the "home away feature" works?
- Are there any particular situations where the "Home away" feature would be useful? If so, what would they be?
- Do you have any concerns about using the Home-away feature?

Follow-up questions:"Thank you. I have some follow up questions" How did your concerns and expectations change after using the device?

- Are you satisfied with the features and controls available in the smart lock?
- Are there any other controls or features you want from smart lock? What are those controls? How would you use those controls?
- How would you change the app to better satisfy your needs?

A.3.3 ***Demographic questions:*** "Thank you so much for participating. Finally we have few demographic questions"

- Your ethnicity:
  (1) Black or African American; not Hispanic
  (2) Hispanic or Latino
  (3) White, Caucasian; not Hispanic
  (4) American Indian/Native American
  (5) Alaska Native
  (6) Native Hawaiian/Pacific Islander
  (7) Asian
  (8) Prefer not to specify
  (9) Other (Please specify)
- What is your age?
- What is your Primary occupation?
- On a scale of 1 to 5 (1 being very weak and 5 being very strong) how would you rate your knowledge of technology in general?
- On a scale of 1 to 5 (1 being very weak and 5 being very strong) how would you rate your knowledge of computer security?
- On a scale of 1 to 5 (1 being very weak and 5 being very strong) how would you rate your knowledge of smart home technology?

A.4 Closing:

"That was all of our questions. Thank you again for participating. If you have any questions, I am happy to answer them. Otherwise, you are free to go."

B Phone interview guide: Owner participants

B.1 Consent:

Participants provide consent to participate in the study online before the phone call.

B.2 Introduction:

"Hi, Thank you for participating in our study. My name is .... and I will be conducting the interview today. Please let me know if you have any questions throughout the interview process."

B.3 Semi-structured interview:

"During the study, you will use a smart doorbell and smart lock."

B.3.1 ***General questions:***

- Do you have the Smart Doorbell or the Lock? What smart doorbell and lock do you have?
- Do you have any other smart devices?
- What smart devices do you have?

B.3.2 ***Smart doorbell:*** " First I want to know about your smart doorbell."

- Tell me about when and why you chose to buy this device.
- I'm interested in what you remember from setting up the device. Did you change any default settings? Did any issues or problems arise?
- How do you currently use the device in your day to day life?
- Any features you are aware of that you don't use and why?
- Any other features you expect from the device? Why?
- How have you made changes to how this device is set up over time? What triggered any changes?

Notification settings:

- What types of notifications do you currently receive from the device?
- Please describe how you configured any notifications you receive from the device?
- Did you ever want to configure what notifications to receive, but couldn't? Why? What factors went into your decisions on what notification to receive and when?
- Is there any additional information you would like to see for the notifications?
- Are there any additional options you would like to have for managing and configuring your notifications?

Event history settings:

- Which types of events does the doorbell store?
- How did you configure when or what the doorbell records as an event. Why?
- Did you ever want to configure when or what the doorbell records during an event but you couldn't. What did you want to configure?
- Are there any additional options you would like to have for managing and configuring the events, specifically video recording?

Video storage settings:

- How do you currently manage your video storage?
- Are there any additional options you would like to have for managing video storage?
- Have you ever deleted a video or wanted to delete a video stored in the doorbell? Why?
- Have you ever shared a video or wanted to share a video stored in the doorbell? Why?

Privacy concern:

- Do you have any security or privacy concerns over the data that your doorbell collects and produces?
- How do you manage the privacy and protection of the data your doorbell records?
- Do you use any specific controls or settings provided? Are there additional controls or settings you would like to see?

Device sharing settings:

- Do you currently share access to the doorbell with anyone or have you shared it with anyone in the past?
- (If yes:)
  - With whom and why?
  - How did you share access? Walk me through what you remember doing to share it.
  - By sharing, what features of the doorbell do you think this person has access to?
  - Do you have any concerns over sharing access to your doorbell with this person?
  - Did you ever want to share the device with someone but couldn't? Why?
  - What other options would you like to have for sharing the device?

B.3.3 ***Smart lock:***

- Tell me about when and why you chose to buy this device.
- I'm interested in what you remember from setting up the device. Did you change any default settings? Did any issues or problems arise?
- How do you currently use the device in your day to day life?
- Any features you are aware of that you don't use and why?
- Any other features you expect from the device? Why?
- How have you made changes to how this device is set up over time? What triggered any changes?

Notification settings:

- What types of notifications do you currently receive from the device?
- Please describe how you configured any notifications you receive from the device?
- Did you ever want to configure what notifications to receive, but couldn't? Why? What factors went into your decisions on what notification to receive and when?
- Is there any additional information you would like to see for the notifications?

- Are there any additional options you would like to have for managing and configuring your notifications?

Event History settings:

- Which types of events does the lock store?
- How you configured when the lock records an event. Why?
- Did you ever want to configure when a lock records an event but you couldn't. Why did you want to configure?
- Are there any other events that you would want it to store?
- How do you currently manage the stored events?
- Are there any additional options you would like to have for managing and configuring the events?

Privacy concern:

- How do you manage the privacy and protection of the data your lock records?
- Do you use any specific controls or settings provided?
- Are there additional controls or settings you would like to see?
- Do you have any security or privacy concerns over the data that your lock collects and produces?

Device sharing settings:

- Do you currently share access to the lock with anyone or have you shared it with anyone in the past?
- (If yes:)
  - With whom and why?
  - How did you share access? Walk me through what you remember doing to share it.
  - By sharing, what features of the doorbell do you think this person has access to?
  - Do you have any concerns over sharing access to your doorbell with this person?
  - Did you ever want to share the device with someone but couldn't? Why?
  - What other options would you like to have for sharing the device?

B.3.4 ***Demographic questions:*** "Thank you so much for participating. Finally we have few demographic questions"

- Your ethnicity:

(1) Black or African American; not Hispanic
(2) Hispanic or Latino
(3) White, Caucasian; not Hispanic
(4) American Indian/Native American
(5) Alaska Native
(6) Native Hawaiian/Pacific Islander
(7) Asian
(8) Prefer not to specify
(9) Other (Please specify)

- What is your age?
- What is your Primary occupation?
- On a scale of 1 to 5 (1 being very weak and 5 being very strong) how would you rate your knowledge of technology in general?
- On a scale of 1 to 5 (1 being very weak and 5 being very strong) how would you rate your knowledge of computer security?
- On a scale of 1 to 5 (1 being very weak and 5 being very strong) how would you rate your knowledge of smart home technology?

B.4 Closing:

"That was all of our questions. Thank you again for participating. If you have any questions, I am happy to answer them."