UNDERSTANDING END-USERS' PRIVACY PERCEPTIONS, CONCERNS, BEHAVIORS, AND NEEDS IN THE SMART HOME

by

Madiha Tabassum

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in
Computing and Information Systems

Charlotte

2022

Approved by:

Dr. Heather Lipford

Dr. Weichao Wang

Dr. Mohamed Shehab

Dr. Weihua Zhou

ABSTRACT

MADIHA TABASSUM. Understanding end-users' privacy perceptions, concerns, behaviors, and needs in the smart home. (Under the direction of DR. HEATHER LIPFORD)

Smart homes are more connected than ever before, with a variety of commercial internet of things devices available. The use of these devices introduces new security and privacy risks in the home and needs for helping users to understand and mitigate those risks by providing them some level of control over their data. For doing so, it is necessary to have a thorough understanding of smart home users' security and privacy perceptions, behaviors, preferences, and needs. My thesis aims to investigate the current state of end-user knowledge of smart home device data practices, available privacy controls, and their security and privacy concerns and behaviors. I have utilized different research methods throughout this exploration, including semi-structured interviews, surveys, and experience sampling studies. The contributions of this dissertation are: 1) it uncovers several factors that contribute to the privacy perceptions, concerns, and behaviors of smart home users, 2) it provides in-depth analysis of the current interface support (or lack thereof) to address end-user privacy needs, and finally 3) it contributes several design guidelines to empower users with their privacy in the smart home.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Internet-connected devices are becoming increasingly popular, especially with the availability of a wide variety of easy to use devices at a reasonable price. According to a recent estimate, 27.5% of US households own smart home devices[13]. These devices provide numerous services such as automation, hands-free control, and intelligent operation of the home. For example, a smart thermostat would be able to raise the temperature so that a user has a warm house when he gets home, while the oven can pre-heat itself so that he can start preparing dinner.

The benefits provided by the smart home are not only limited to convenience but also include a wide range of services offered to the residents. For example, one application of a smart home is security and surveillance where inhabitants can monitor their house using smart cameras, get notification of any break-in, or any other emergency in the house, such as water leakage. Overall by providing all of these services, the smart home is helping occupants to reduce costs and save money with a better living experience in the home.

Though smart home devices provide numerous services to enhance the comfort and experience of the inhabitants, these devices also expose the home occupants to many security and privacy risks. Smart home devices continuously collect and transmit a vast amount of information about users and their environments to provide these services, often without explicit knowledge or consent of the users. Such invisible

and pervasive data collection in high volume by these sensors, which are often privacy sensitive, can seriously jeopardize end users' privacy in general. For instance, it is possible to make a very accurate profile of users and their behaviors from this information, which can lead to stigmatization, embarrassment, discrimination, etc. Shopping habits have already been analyzed and used by insurance companies to set the premiums[15]. Moreover, the companies that are legally collecting this information may share it with third-party advertisers. In a study with 81 smart home IoT devices, researchers found that 72 of the devices share data collected from the devices such as IP address, usage habit, location, etc [12]. The data was shared with third parties that are not related to the original manufacturer. Often, these third-party entities reside outside of the country where the devices are located.

In addition to the risks from the collection, use, sharing, and retention of user's data by the smart home companies, privacy risks can also come from the multiple stakeholders who have access to these smart home devices. For instance, smart home devices are shared by multiple people who live in the house. Lack of boundary regulation in these devices can lead to violations of privacy by other household members. For instance, parents prefer the smart lock to create a photo log when their teenagers come home. However, teenagers consider it privacy-invasive and prefer their parents to have access to only text logs or no logs at all[83].

Apart from the people who live in the house, there are other stakeholders as well who have access to smart home devices. For example, family and friends visit the house, house cleaners and contractors help with maintenance, and neighbours keep an eye out for emergencies. Lack of transparency and control over sharing these smart

devices may lead to unintended sharing of sensitive information, for instance, visitors with temporary access to the smart camera looking at previously recorded videos.

Today, with all the Internet-connected things, the security and privacy of our home is now becoming reliant on the security and privacy of the digital devices that reside within it. It could be argued that data collection and sharing are not new in the context of social media, search engines, or online web applications. However, with time, people have formed opinions and practices through their experiences using these mediums. For instance, people remove cookies from the browser, use websites with https connections, use VPNs to hide their location or do not share very personal information over the social media.

The smart home is a relatively new frontier, with a very complex ecosystem where a wide variety of personal data is collected from users' homes. In contrast to other contexts where data is collected when users are actively using the websites or applications, smart home devices blend into the home environment, become invisible to the home occupants and continuously collect data in a pervasive manner. Research on social media and the internet has demonstrated that users are uncertain about how their data is collected, shared, and stored online among different stakeholders even though they are concerned about it. It will get worse in the smart home with the ubiquitous data collection by things inside the home.

Many security and privacy problems that are prevalent online occur because the designers do not consider end-users' perceptions, needs, and abilities when developing the system. For instance, users fail to encrypt their email using modern PGP clients because they have an erroneous perception of how encryption works and the interface

does not provide enough support to change their perception [76].

Hence, I believe it is important to understand how the inherent privacy issues of smart home devices impact end-users. The mechanisms to aid users with security and privacy in the smart home should consider end-users' perceptions, concerns, and needs to be usable, effective, and adopted by the consumers. Therefore, my research presents an in-depth examination of the end-users' perspectives on security and privacy in the smart home and current interface support (or lack thereof) to aid their needs.

1.1 Thesis Statement

End-users need to understand the risks that come with smart home devices and be aware of the protection practices so that they can reason about the trade-offs and take actions required to mitigate those risks. Nevertheless, smart home users are not sufficiently aware of the sensing capabilities of these devices, the data that are being collected and shared by these devices with different stakeholders (device manufacturers, third-parties, other users of the device). Current interfaces fail to provide users with adequate awareness of the data practices and fine-grained controls to protect their desired data and social privacy in the smart home.

1.2 Research overview

An important aspect of establishing design requirements for helping users with their security and privacy practices is to understand their current perceptions of risks. Several works [88, 91] examined the perceptions of users of consumer devices that they use in their own homes. These studies, primarily of technically skilled smart home early adopters, examined general privacy and security perceptions [88]

and concerns regarding specific data collection entities [92] in the smart home. They found that users' perceptions of smart home security and privacy threats are often influenced by their experiences in other computing contexts and the benefits they received from the devices. However, an in-depth understanding of users' perception of data practices – how devices collect, send, and share data and how that influences their security and privacy practices in the smart home is still lacking.

A number of studies also looked at end-users' practices and concerns around the shared use of devices inside the home [39, 34, 35]. They found that users have complex access control preferences, which are often guided by the type of device, relationship with the sharee, users' awareness of device capabilities, and different contextual factors such as time, location, etc. While these studies looked at smart home device sharing in the home, homeowners may also wish to share remote access to their devices with other people who do not live with them. Neighbors could check on a home in case of a fire or burglar alarm. Neighbors may also want to share access to each other's security or doorbell cameras to monitor community safety and security [75, 23]. Users' device sharing practices, concerns, and preferences and how they manage their social privacy in this context have not been revealed by the prior studies.

Moreover, these studies retrospectively ask users about their thoughts and practices of data and social privacy. Hence, prior research failed to capture end users' in-situ security and privacy considerations and needs, what factors elicit those considerations, what mechanisms users utilize to alleviate their concerns, and how the current interfaces support users in the process.

Hence, the focus of this thesis is to explore end-user knowledge and identify factors

that influence their privacy concerns, preferences, and needs in a smart home and how the current interfaces accommodate users with their security and privacy needs. As such, I am investigating multiple research questions:

- What are end-users' perceptions of data collection, sharing, storage, and use by smart home devices and their manufacturers? How do these perceptions and concerns relate to users' privacy and security considerations and mitigation strategies?
- What are smart home device users' device sharing behaviors and how do the current interfaces support end users' device sharing needs?
- What are end users' concerns regarding managing their privacy in the multi-user environment? How do end users' sharing practices relate to their concerns?
- What privacy considerations do end users have as they use these devices? What factors elicit these considerations? What decisions and actions do they make at that moment, and what additional support do they need?
- How do end-users perceive privacy controls available in different smart home devices? What considerations do they make while configuring those controls? What security and privacy behaviors (or lack thereof) do they exhibit to support those considerations and their implications?

I investigate these research questions through a variety of user research methods that provided a comprehensive understanding of end user's considerations in a smart home.

In chapter 3, I have conducted a qualitative study to understand users' views of their smart home data privacy. For instance, I investigated users' perceptions of the data that is generated, collected and shared, and their related security and privacy concerns and mitigation behaviors in the smart home. Our study highlighted participants' uncertainty and desire to have greater control over the collection, sharing, and removal of their data. However, our findings also suggest that participants do not even know or are skeptical about the controls they already have in the smart home devices.

In chapter 4, I turn to understand how people share smart home devices with multiple people and keep their desired privacy. Specifically, I looked at smart home device sharing and access control beyond the home through the combination of a survey and interview study. We found that people are often uncertain about the access they are sharing with people for different devices, as well as confused about the devices' access control capabilities. This study provides insight into the range of potential uses of the remote sharing capability, as well as the needs for homeowners to monitor and control such access.

Privacy is contextual, and users' concerns, preferences, and decisions may change based on the surrounding context. The nuances of privacy problems are often not revealed when participants are retrospectively asked about it. Hence, in chapter 5, I have conducted an experience sampling study for two weeks in several smart home households to understand what data and social privacy concerns there are in the context of smart devices depicted from users actual behaviors. I have used a mobile application named PACO, where participants logged their feelings and reactions to

any privacy considerations they had as they were using these devices in their day-to-day life. After the initial data collection period, I conducted follow-up interviews using the recorded events as prompts to get a deeper understanding of users' considerations, their actions, and needs. The study identified several factors that elicit end-user privacy considerations and the support they need at that moment.

We found in our previous studies that while people say they want more control over their data in the smart home, they are not even aware of the controls provided upfront by the device manufacturers. For example, we found that some participants who have an intelligent voice assistant (i.e., Amazon Echo) do not know there is an option to view and delete their recordings[80, 60]. Before designing new security and privacy mechanisms, it is important to understand how users use the existing mechanisms, what considerations they make, and determine the gaps where devices are failing to provide desired awareness and controls. Hence I have explored users' perception, considerations, and decisions while using the privacy mechanisms in the smart home devices (centering on the smart doorbell and smart lock) in chapter 6. I have conducted an interview study with both owners and non-owners of these devices. This study demonstrates that configuration decisions have implications on users' data privacy and the need for mechanisms to inform users of such implications while making those decisions.

Finally, in chapter 7, I will summarize the findings from all of these studies, and discuss the implications, considerations and guidelines for developing privacy-preserving smart home systems.

1.3 Contributions

In summary, the contributions of this research will include:

- Provide an in-depth understanding of end-users' perceptions and concerns of smart home device manufacturers' data practices.
- Provide a detailed understanding of end-users' device sharing behaviors, concerns, and needs.
- Portray in-situ security and privacy considerations, behaviors, and needs of smart home users and identify factors eliciting considerations.
- Detail a set of design implications and guidelines that will contribute to the development of effective security and privacy mechanisms for the smart home.

CHAPTER 2: BACKGROUND

Smart home devices bring a lot of convenience and comfort to the lives of home occupants. However, because of the proximity, ubiquity, and unobtrusiveness of these devices, they also open smart home users up to many security and privacy risks. In this section I discuss the existing human-centered research in the area of data and social privacy and security in the smart home.

2.1 Smart Home and data privacy

The smart home is a combination of embedded sensors, smart devices, network devices and gateways that interact with each other to collect the state of the home environment, the activities and behavior of the occupants and take appropriate actions to make their living experience more effortless and pleasant. Despite the benefits of a smart home, information privacy became a paramount concern in recent years with the increasing use of electronic data and internet connected devices at home. Information privacy refers to individuals' control over the collection, use, and dissemination of their data by different entities. As smart home devices continuously and ubiquitously collect, transmit and process information about the house and the inhabitants with limited control over the data, information privacy is one of the most critical issues and key adoption barriers of the smart home [64].

With the varieties of sensor data these smart home devices are collecting, it is now

possible to identify and track people even in their private spaces and learn about their family dynamics, preferences, behaviors etc. We are entering into a new era of surveillance with the smart home devices. Sensors are augmented in daily life that are continuously sensing the environment and the house. These devices can take the form of a regular household object with hidden sensors. For example, the "hello barbie" doll looks like a typical kids toy [7] and "Alexa" looks like speakers, but both have ability to understand audio and talk to people. As such devices blend into the households, inhabitants may end up sharing more data than they normally would if they were aware more consciously of the presence of the device.

A lot of information can also be inferred about the occupants even from the meta-data these devices are collecting, i.e, network traffic rates from a Sense sleep monitor revealed consumer sleep patterns, network traffic rates from a Belkin WeMo switch revealed when a physical appliance in a smart home is turned on or off, and network traffic rates from a Nest Cam Indoor security camera revealed when a user is actively monitoring the camera feed or when the camera detects motion in a user's home [19]. It is considerably alarming as internet service providers(ISP) will be able to view this data and last year U.S. Congress voted to allow ISPs to use and sell the data collected from their customers' network traffic [9].

Therefore, the threat of profiling will increase because of the large amount of data collected by the smart home devices and the way they collect information about previously inaccessible parts of peoples' private lives. The smart home device vendors can now create a reasonably accurate profile of a user and use that for advertising. For instance, Amazon and Google have patented to use the digital voice assistant

to extract keywords from the ambient speech and use that to provide relevant advertisement [8]. Thus smart home devices exacerbate the power imbalance between companies and users by collecting private information from a user's home. Home users are still struggling with implementing best practices to secure their privacy for computer systems [84]. Internet connected objects bring new complexity that they can not manage. The information that can be inferred about the occupants from the smart home devices can be used to manipulate their behavior; for instance, users can be influenced to buy a certain product they do not want or think of buying or nudged to spend more [67]. We have already seen the manipulation of US voting behavior in 2017-2018 by exploiting the facebook profiles of 87 million users [6]. Such circumstances will only grow worse with the advent of smart home devices.

Moreover, the only way for users to know about what data is collected and how that is used is from the privacy policy or the end user license agreements provided by the vendors. Yet, these documents are long and full of jargon. The complexity of understanding the privacy policy for only one device can be overwhelming for a regular user. In the smart home, a lot of devices and applications interact in complex ways and understanding such policies for each of those can be beyond the capability of most users. Furthermore, a trend of being less transparent and informative about the data policies is emerging among the manufacturer of the smart home devices, which makes the problem more severe. Peppet investigated twenty IoT devices, including the Nest thermostat and home monitoring systems, and found that none of the device manufacturers provided privacy and data related information in the box [73]. All the device manufacturers have privacy policies on their website; however for some of them

they only account for the website data usage policy, not data collected by the device sensors [73].

Integration of the myriad of smart devices in home environments introduces new and unique questions about data collection and use that may be challenging for end users. With this new domain comes new risks to users' security and privacy. And new questions as to how to support users in understanding, reasoning about, and mitigating those risks. As a first step to developing privacy-preserving services in this complex system, it is necessary to understand users' expectations and concerns regarding their privacy in this continuous sensing environment. In the following section, I will discuss related works that investigated privacy concerns, expectations, and factors that impact privacy preferences with respect to smart devices.

2.2 Concerns, expectations and preference about data privacy

End users' concerns about their data privacy have been explored heavily in the context of the Internet and software. Usually, these have been explored from a task- or tool-specific perspective, such as understanding of the operations of WiFi networks, general home computers or firewalls. For example, Kang et al. explored users' perception of the Internet in general [45], also asking users about their perceptions with regard to data practices on the Internet. Though they found that participants with a more accurate understanding of the Internet have more awareness of who can have access to their personal data, most of the participants had a great deal of uncertainty and concern about how their data will be used. Wash et al. found in an interview study [84] that home computer users are often unable to make better security and

privacy decisions primarily because of the lack of relevant knowledge and skills. We believe many of these findings will carry over into the smart home. Yet, the smart home is more complex, and is more integrated with people's personal lives, introducing new questions and concerns about personal information collected by the smart devices.

A number of researchers have examined end user concerns, expectations and preferences with smart devices in the home. However, early work relied on prototypes or probes within homes to examine users' reactions and perspectives, given the limited availability and adoption of smart home devices at the time. For example, Choe et al. [26] used sensor proxies in 11 households as a cultural probe and found participants had concerns about unintended use of their data and the possibility of data exfiltration. They also found tensions between different members of a household around the use and adoption of such in-house sensing applications. Worthy et al. [85] installed an ambiguous Internet of Things(IoT) device in 5 participants' homes for a week and found that trust in the entities that use the data (in this case, the researchers) is a critical factor in the acceptance of the smart device. Montanari et al. [70] invited 16 participants to interact with two smart home devices during the study session and found that users are primarily concerned with the ownership of their data.

A number of studies have also examined the role of context in users' comfort of sharing IoT-related data. These studies reveal that privacy concerns are indeed contextual, depending on a variety of factors such as the type of data recorded, the location where it is recorded, who the data is shared with, the perceived value of the data and benefits provided by services using that data [49, 71, 55, 59, 37, 20, 54].

Naeini et al. [71] used vignettes to study many of these factors with over 380 different use cases across 1,000 users. Their results indicate that people are most uncomfortable when data is collected in their home and prefer to be notified when such collection occurs. Similarly, a survey study by Lee and Kobsa [55] found that monitoring of users' personal spaces, such as their homes, was not acceptable to participants, as well as monitoring performed by the government or unknown entities.

Other studies have found that people are most concerned with certain types of data, namely videos, photos, and bio-metric information, particularly when this information is gathered inside the home [56, 18, 71, 55, 30]. In another large vignette study, Apthorpe et al. [20] found that participants' acceptance of data collection and sharing was dependent on both the recipient of the information and the specific conditions under which the information was shared. Their results also suggest that users' privacy norms may change with continued use of specific devices. However, results of a different vignette survey by Horne et al. [42] suggest that those changes are not always towards more acceptance of data-sharing.

Abdi et al. followed a similar approach to identify acceptable information flows with a smart personal assistant [16]. They found that the recipient of the data is the most influencing factor in determining the acceptability of the information flow. Barbosa et al. also have conducted a contextual survey involving data type, the 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 [22].

Each of these studies examines fine-grained contextual factors through survey meth-

ods of potential use cases of smart home devices. Though such methods can be helpful to get a deeper understanding of users' expectations and how they make different tradeoffs in the smart home, we believe it may not be a reliable method to explore the effect of the different factors in users' expectations and preferences. With this methods users either imagine themselves in a specific situation or recall their experience with smart home devices, which may not always align with their expectations when they actually experience that situation.

With widespread adoption, several studies have recently examined the perceptions of users of consumer devices that they use in their own homes and found less concern by actual, regular users. Lau et al. [52, 53] conducted a combination of a diary and interview study with 17 users and 17 non-users of smart voice assistants. They found that the lack of trust and perceived utility are the main reasons for not adopting the device. They also noticed that adopters of the voice assistant have an incomplete understanding of the privacy risks and rarely use existing privacy controls.

Zeng et al.[88] conducted an interview study of 15, primarily technical, smart home users and observed limited concern among participants about the potential improper use of their data. They also found that even relatively technical participants have an inaccurate or incomplete understanding of smart home technology, resulting in incomplete threat models and adoption of insufficient mitigation techniques to resolve potential threats. Zheng et al. [92] interviewed 11 technologically skilled smart home users on their reasons for purchasing smart home devices and the perceptions of privacy risks from these devices. They found that users' concerns over specific external entities (i.e. government, manufacturers, internet service providers and advertisers)

are influenced by the convenience they get from the device and those entities. However, Hanly 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 [38].

Despite these findings showing concern regarding data collection in the home, many users are installing smart home devices that do collect and share some information. These prior studies have not revealed what adopters of current devices think is actually occurring, and their comfort and concerns with those practices which I believe are imperative to understand end users' privacy in the smart home.

2.3 Smart Home and Social Privacy

Smart home devices are generally shared by multiple people (i.e., roommates [58], guests [44], neighbors [23], teenagers [83], and kids [77]) who access these devices for different reasons. These devices facilitate interactions between multiple people and objects, resulting in potential benefits as well as privacy concerns that go beyond an individual. For instance, spying by the admin user who set up and controls the devices on other occupants in the house may violate users' general expectations of privacy. Moreover, there are also risks of sharing sensitive information(i.e., video recording) with other people (i.e., visitors) if the access rights being shared are not transparent to the users.

People, in general, have complex access control preferences for sharing digital devices in their house [25, 65, 58]. While residents may trust each other, prior research has found that they also prefer to keep separate profiles in their digital devices [25] and

often try to implement complicated policies using makeshift methods, especially when their mental model of access control is misaligned with the actual system [65]. Smart home device users may need flexible and rigorous access control policies as well, since these privacy-sensitive smart devices often get shared among multiple stakeholders with different trust and social relationships.

2.4 Concerns, expectations and preference about Social Privacy

Several projects investigated smart home access control policies by studying early adopters, prior to the current wave of smart home devices. In an interview study with thirty-one smart home users, Brush et al. found that people consider access control in terms of a few simple groups: adult residents, kids, and guests, and want to provide temporary access to guests [24]. They also found that access-control policies based on time (e.g. blocking children from watching TV at night) and measures for restricting highly sensitive devices such as cameras and locks were highly desirable among users [31].

In an interview study with 20 non-users of a smart home, Kim et al. sought to understand how people would set access control policies for different devices in their homes [47, 48]. Based on participants' stated desires, they suggested three possible dimensions for an access control policy: physical presence, logging, and the capability of asking permission. Ur et al., investigated a first-generation Internet-connected lighting system, bathroom scale, and door lock and found that they lacked a mechanism for users to monitor which accesses are shared. They also reiterated the challenge of defining an easy to use access control policy, even for these comparatively

simple devices [82]. Rendall et al. however, pointed out that as control systems become more complicated, people feel that they actually have less control over their devices [74]. Keeping that in mind, Kostianinen et al. tried to introduce an access control policy for smart home networks limited to family members, which would pose a minimal burden on the end-user [51].

Though these initial studies looked at different aspects of smart home access-control, both the consumer landscape and the devices have changed significantly in recent years. Most smart home IoT devices now offer some form of controlled sharing among users. For instance, the Ring doorbell offers a feature that allows the owner to add a user to the doorbell, providing access to a predefined set of capabilities [41]. The Nest thermostat gives users the option to add a family member, providing them full access to the device [40]. Many devices offer similar features.

Thus, multiple recent studies have focused on multi-user sharing, and have found tension in the use and control between people in a smart home [36, 43, 89]. 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 [50]. Such a lack of involvement creates the potential for abuse from the admin user [88, 66, 57].

In a diary study with 20 participants, Garg et al. noticed that end-users' device sharing practices are often influenced by their lack of understanding of the device's behavior and well as the inability of the devices to recognize the context of use

inside the house [34]. In a large scale vignette study, He et al. [39] found that home IoT users desired different access control capabilities for different functionalities, even within a single device. They advocate for more complex access control policies that take into consideration the relationships among the stakeholders, specific device capabilities, and different contexts such as time, location of the device and people. Recognizing these design principles, for instance, the need for role and location-based access controls, Zeng et al.[90] developed a prototype smart home app and evaluated it with seven households in a month-long in-home study. However, they found little use of nuanced access control by the participants, either because of the complexity of setting up the policy or the strong trust among the household members.

Several other studies looked at the perspective of the non-household members, aka bystanders (visitors, neighbors, etc.) [62, 87, 28]. 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 [62]. 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 [87]. 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 [28].

Many of these prior studies focus on sharing devices for those within a home - other residents and visitors. Yet, as prior work in the digital neighborhood watch demonstrated [24], smart devices can enable communities of users to support each

other in the safety and security of their homes, not just residents themselves. And users now have the ability to share control and access to their smart home with anyone over the internet, even with people who do not live with them. While this technical capability exists, research on whether and how people would want to share this remote access is lacking. More research needs to examine the benefits and concerns that could arise when devices are used within trusted communities of people.

2.5 Existing privacy preserving frameworks and strategies

There have been several strategies proposed in the literature to address end users' data collection related concerns and help them to preserve their privacy in IoT and the smart home. Fernandes et al. [56] proposed a system, Flowfence, to block the unintended data flows in IoT applications. Flowfence requires consumers of the sensitive data to declare intended data flows. It then enforces only those data flows and prevents any other flows. Mehrotra et al. [57] designed two systems that help to study the privacy risks emerging from the sensory data and to design the corresponding protection mechanisms in the actual system context. Rahmati et al. [58] developed Tyche, a risk-based permission model for the smart home. They divide the smart device operations into low, medium and high-risk groups. With Tyche, users will be able to give risk-based, i.e. low, medium or high-risk permission to smart device applications.

Ukil et al. [59] proposed a privacy management scheme that enables users to estimate the risk of sharing data from their smart energy system, i.e. smart meters. Lederer et al. presented five pitfalls that designers should avoid especially in designing

a user interface for managing privacy in ubiquitous computing [60]. These pitfalls can lead to negative implications for individual privacy. Egelman et al. [61] employed a crowdsourcing approach to design several privacy icons to communicate specific data collection in the ubiquitous sensing platform. He et al. identified several default access control policies for the smart home through a 425 participant online survey study [62].

One of the shortcomings with the existing privacy interfaces is that the implementation of those were discussed from a developers point of view, but no evaluation was reported on how end users perceive such interfaces and their implications. Some other interfaces and methods were developed only to support researchers and designers to create privacy-protective measures for the internet of things. Many of these works also did not take into account the unique challenges of the smart home. While the existing research is a useful step toward implementing privacy-preserving technologies on the internet of things, more research is needed especially in the domain of the smart home to enhance non-tech savvy user perceptions of security and privacy controls and their ability to manage personal data.

2.5.1 Awareness, notice and control mechanisms

Privacy notice and awareness mechanisms are critical to inform users of the privacy issues and risks to help them make decisions. There have been multiple research efforts to examine awareness mechanisms in the smart home context. Emami-Naeini et al. have proposed an IoT Security and Privacy Label [32] 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, data sharing practices, 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, [10]. 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 [43, 69]. 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 [43].

Researchers have also aimed to accommodate user's privacy needs through proposed privacy features and interfaces [29, 90]. 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 [29]. 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 [86]. 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 [60]. 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 [53].

Several studies have looked more specifically at the access control mechanisms in the smart home[82, 39, 90], examining the design needs and uses for people sharing devices with others. 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 [90].

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 [61]. Furthermore, Feng et al., introduced a design space taxonomy for privacy choices [33]. They present five key dimensions: choice type, functionality, timing, channel, and modality to consider for providing meaningful privacy controls in IoT.

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.

2.6 Research Extensions

In this chapter, I have discussed the smart home issues from the context of end users' data and social privacy. Though existing literature provides us with useful

insights about end users' privacy and security concerns, preferences, and different factors that define the privacy norms in the smart home context, I believe there are still a number of questions that need to be addressed to develop a privacy-preserving smart home. For instance, a detailed understanding of end-users' perceptions of data privacy, how they maintain their social privacy, what are their security and privacy needs in real-time, and how the current interface supports these needs. I am contributing to the state of the art by exploring these research questions to provide the research community with a more coherent picture of what end-user privacy means in the smart home.

CHAPTER 3: EXPLORING END USERS PERCEPTIONS OF SMART HOME DEVICE DATA PRACTICES AND RISKS

The results from this study have been published in the Symposium on Usable Privacy and Security (SOUPS), 2019 in California, USA. Full citation can be found here [80].

3.1 Introduction

Smart home devices greatly expand the types and amount of information about ourselves and our environments that can be collected and shared. Consequently, new questions emerged as to how to assist users in preserving their preferred level of privacy in this passive and ubiquitous information gathering ecosystem. As such, a number of researchers have examined end-users concerns, expectations, and preferences with smart devices in the home. Early work relied on prototypes or probes within homes to examine users' reactions and perspectives [2,3]. They found that trust of the entities that are receiving the data play an important role in the adoption of such in-home sensing devices. They also found tensions between the different residents surrounding the use and adoption of such devices.

Later work[4,5] examined the perceptions of users of consumer devices that they use in their own homes. Studies have found that users' perceptions of how smart homes work and the potential threats are often incomplete and inaccurate, even for the relatively technical consumers. Users' perceptions of smart home data practices and threats are often based on their experiences in other computing contexts, which

results in the adoption of insufficient mitigation techniques to resolve threats unique to smart home devices. However, none of this prior work looked specifically at user understanding of data practices – how devices collect, send and share data – which we believe is critical to understand users' perceptions of security and privacy. In addition, this prior work relied primarily on early adopters who are technically knowledgeable, which limit the generalizability of their results.

Hence, we have conducted a drawing exercise and semi-structured interview with 23 participants who have experience living with multiple smart home devices. We focused on recruiting both more technical participants who installed their devices, as well as non-technical users who were not involved in the installation process. We investigated users' mental models of data flows in their smart home, their overall perception of the different aspect of companies' data collection, use, storage, and sharing practices, and their security and privacy concerns and behaviors. Insight gained from this study helped us to yield recommendations for smart home designers, researchers, and policy-makers to provide improved awareness and control of data collection practices and protection strategies, considering the perceptions and capabilities of general smart home users.

3.2 Methodology

We conducted a semi-structured interview study and drawing exercise of smart home residents to elicit their mental models of the data practices of smart home devices, along with their perceived security and privacy risks and concerns.

ID	Gender	Age	Education	Profession
ID1*	M	21-30	MS: Computer Engineering	Grad student
ID2*	M	21-30	BS: Computer Science	Programming consultant
ID3*	M	21-30	Juries Doctorate	Attorney
ID4*	M	31-40	Doctorate: Medicine	Product manager
ID5	F	21-30	BS: Biology	Banking
ID6*	M	61-70	BA: Urban Planning	Retired computing professional
ID7*	M	51-60	Associate Degree: Arts and Science	Computing professional
ID8*	M	41-50	Diploma: Media Arts	Network engineer
ID9*	M	31-40	BS: computer science	IT sales
ID10	F	31-40	MS: Kinestheology	Unemployed
ID11*	F	21-30	MS: Kinestheology	Clinical researcher
ID12*	M	31-40	Post Graduate: Chemistry and Physics	Business entrepreneur
ID13*	F	31-40	MS: educational counseling	Education administration
ID14	M	51-60	BA: Criminal Justice	Banking
ID15	F	31-40	BA: Russian	Human Resource
ID16	F	21-30	Bachelors: Biology and Psychology	Insurance verification specialist
ID17*	M	31-40	Masters: Sociology and Applied Research	Higher education administrator
ID18	F	21-30	Bachelors: Elementary Education	Fifth grade teacher
ID19*	M	31-40	High School	Customer Service
ID20	F	61-70	Bachelors: Accounting	Accountant
ID21	F	61-70	College	Retired
ID22	F	51-60	BA: Practical Civilization	Administrator: call center
ID23*	M	21-30	BS: Biomedical Sciences	Graduate student

Table 1: Summary of the participants. * represents the person involved in installation.

3.2.1 Participants

We sought participants who are regular users of smart home devices and thus had mental models of the smart home ecosystem informed by their usage. We recruited participants with at least three devices, similar to Zheng et. al. [92]. We explicitly recruited some participants who did not install the devices themselves (such as family members) to find people who are not as tech-savvy and may have different privacy perceptions. The participants were recruited through advertisement on Craigslist, and IoT-related Reddit communities. Potential participants were asked to fill in a pre-screening survey answering what types of devices they have in their home, whether they set up the devices by themselves as well as demographic information and email

Type of device	Count	Users' perception of information collection
Intelligent voice assistant	20	Voice interaction (20); Usage (10); Account info (5)
Smart light	16	Patterns & usage (11); State of the lights (10);
Smart plug and switch	13	Account info (5); Home location (2)
Smart camera/doorbell	11	Video (11); Home location (4); Usage (3)
Smart thermostat	11	Temperature (10); Usage (5); Energy use (3); Account info (2)
Hardware hub	8	Usage (6), Location (3), Other devices in the network (2)
Streaming device	8	Viewing history (4); Account info (3)
Other devices: Smart TV (5), Leak sensor (4), Smart Doorlock (3), Open/close sensor (3) Motion sensor (3), Smoke detector (2), Smart media hub (2)		

Table 2: Summary of the devices owned by participants. Numbers in the parentheses are number of participants

address. We recruited participants until we felt we had a sufficiently diverse sample, and then found we reached saturation (i.e., no new codes or new information attained) during analysis, and hence did not seek additional participants.

We recruited a total of 23 participants (see table 1). Six of them had a background in computer science, either as a student, or as a computing professional or both. 13 participants were male and six were more than 51 years old. All participants were living in the United States, except one in Canada and one in Sweden. 11 participants installed and manage the devices in their home, 3 participants installed some of the devices and 9 were not involved in the installation and configuration process at all. Not surprisingly, participants who installed their devices self-reported a higher level of familiarity (statistically significant) with technology and smart home security and privacy, than users who did not perform the installation. We acknowledge that there can be tech-saavy non-installers; however, we did not find such participants in our study sample.

3.2.2 Procedure

The researchers contacted selected participants via email to schedule a phone or Whatsapp interview. The interview was semi-structured, with a set of basic questions that were varied depending on the response of the participants. The interviews were recorded via Google voice or an external audio recorder. Interviews lasted on average an hour and participants were given a $10 Amazon gift card for participating. The study was approved by our university Institutional Review Board (IRB).

We started the interview by asking general questions on what smart home devices participants have, and how they use and control those devices. Participants were then instructed to perform a drawing task to elicit their understanding of how their smart home works. Participants were asked to "draw how these devices collect information and how that information flows between the devices and any other involved entities" and to explain their thoughts verbally during the drawing exercise. This has been used as an effective method in capturing mental models in the literature [88, 45]. We utilized remote Google drawing as it was accessible to most of the participants and has been used previously for remote drawing tasks [88]. This could impact the drawings, as the participants utilized shapes and lines rather than free-form strokes. However, participants explained their drawings as they were creating them, similar to an in-person interview. Only 2 participants sent pictures of their drawings via email during the interview because they felt more comfortable drawing on paper. However, after sending the drawing, participants extensively talked about what they drew. We recognize that a drawing exercise in a remote interview is challenging, but we feel the

trade-off in finding a more diverse sample was worth it.

We then focused on participants' perceptions of data practices, asking the participants what data they think the smart home devices they own are collecting and where these devices are sending and storing that data. Participants were then prompted to discuss who they think has access to their data and how it is being used, as well as whether the devices are sharing the information, with whom and for what benefit.

Next, we asked participants if they have any concerns regarding those data practices. We then asked them what they do to mitigate their concerns and resolve the threats that they think arise from using their smart home devices. We discussed what controls the participants believe they currently have over the data the devices are collecting, what controls they expect to have and their expectations regarding the security of their data. Finally, we collected participants' demographic information at the end of the interview.

3.2.3 Data Analysis

We transcribed the interviews and used an inductive coding process to analyze the data. Two researchers independently coded the interviews of five participants and came up with a list of common themes and patterns. Then the researchers compared and merged the themes and agreed on a shared codebook with 15 structural codes divided into 60 sub-codes. The two coders then independently coded the rest of the interviews. After all the interviews were coded, the researchers met and discussed the codes, resolving any disagreements caused by misunderstanding the codes. We tracked the disagreements and the Cohen's Kappa, a measure of inter-rater reliability,

was calculated at 96.37.

The participants' drawings and related verbal explanations were separately analyzed by the primary author, who clustered similar drawings and conceptions into two emerging categories. The clustering was performed based on the complexity of participants' mental model about both the physical architecture of their smart home and corresponding data flows throughout the system. These categories were then discussed among all the authors, and used to examine differences between participants' perceptions throughout the results.

3.2.4 Limitations

As with similar interview-based studies, we consider sample size to be the biggest limitation of this work. We can only provide limited qualitative results on the posed research questions, yet hope that those revealed patterns can be used in formulating further studies of more representative populations and to inform design. We also believe that the participants, even the non-technical ones, that we interviewed are still the early adopters. They are clearly well educated, and likely of high socio-economic status. They also value the benefit of the devices and decided to have them in their homes. Hence, they have already made the decision that the trade-off is worth the risk; therefore they may not have as many concerns as non-adopters. Thus, these results may not generalize to a broader consumer base who will adopt smart home devices in the future. Still, we hope that many of these patterns would be found in a more general population as we found many of the perceptions did not differ between participants of different levels of expertise. Another limitation is that

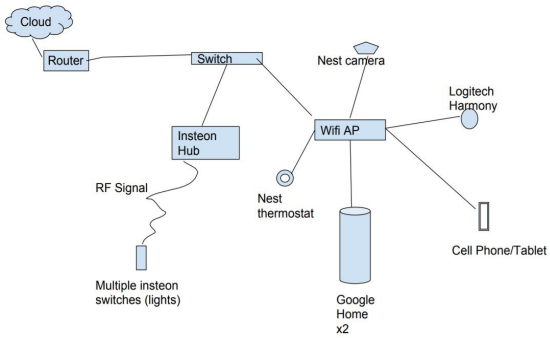
this was a one time interview, which entails the risk of missing participant concerns that could be discovered in, for instance, a longitudinal study. Finally, almost all of our participants are from the U.S. and may have a different perspective about privacy from other regions. Because we have only two participants from other countries, it was not enough to identify those differences.

3.3 Results

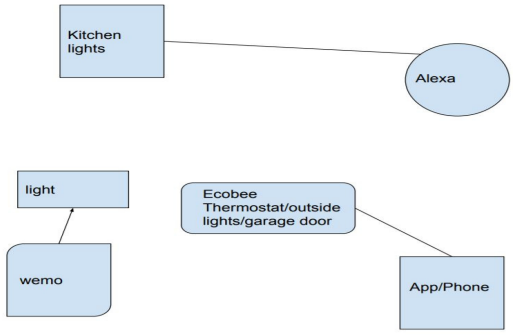
Our study goals are to examine users' perceptions and concerns of the data practices of smart home devices. First we describe the devices they have and use, then present the results of our analysis of participants' mental models, their perception of manufacturers' data practices and their related security and privacy concerns and behaviors. Please note that the numbers reported below are not meant to convey quantitative results, but simply reflect the prevalence of particular themes within our experimental sample.

3.3.1 General Use of Smart Home Devices

Participants own a wide variety of internet-connected devices, including integrated devices (lights, thermostats), home monitoring and safety devices (security cameras, door locks), home appliances (vacuum cleaners, smart refrigerator), and intelligent personal assistants (Google Home, Amazon Echo). We summarize the common devices in Table 2. Participants use these devices in a number of ways. The most frequently mentioned ($n = 11$) use case is household automation (automatically turn on/off the lights, adjust the temperature, etc.), followed by remotely sensing and controlling the home ($n = 10$) (i.e. to turn on/off the lights, check on pets). Another use



(a) Advanced model (Id9)



(b) Service-oriented model (Id20)

Figure 1: Drawing of participants with different mental models

case ($n = 9$) is increasing the security or safety of the house (by notifications of conspicuous sounds in the house, water leakage, etc.). Other less frequently mentioned use cases are energy saving and help with household chores.

We also asked participants how they interact with their devices. Participants use several different methods, often in combination, depending on the location of the user within or outside of the home, as well as the type of device and its compatibility with a controller. Almost all participants ($n = 21$) have a central controller set up, i.e. either a smart voice assistant, hardware hub, an app (e.g. Apple Homekit) or a custom-made controller using the Raspberry Pi. For 13 participants, voice is the primary method of interaction when they are home, utilizing either Amazon Echo or Google Home. Some participants also mentioned setting up triggers based on other

sensor data or timers to make devices fully automated (i.e. using IFTTT services).

3.3.2 Mental Models of Smart Home

Our analysis shows that participants with different technical backgrounds and experiences with the devices have different mental models of how their smart home works. We asked users to describe how data flows in their smart home, and participants chose different ways to express this. We grouped based on similarity of participants' understanding of how devices are connected and how information flows in the smart home and this resulted in our categorization. Two models emerged: advanced (9 participants) and service-oriented (12 participants), based on participants' drawings and verbal explanations of their smart home. We did not include Id6 and Id21 in our categorization. The recording of Id6's drawing explanation was distorted, and Id21's spouse was helping her with the drawing during the interview.

Participants with the advanced model consider their smart home as a complex, multi-layer system. These participants have a reasonable understanding of the logical topology of the smart home, connection mechanisms (Ethernet, WiFi, ZigBee/Z-Wave) and the role of some network components (routers and hub) in communication (Figure 1a). All the participants with this model also discussed how data flows back and forth between the devices and servers in the cloud when interaction happens. For example, Id19 said,

" *When its (Echo) not being used, it is just waiting for one of four trigger words and when that triggers, then it opens up the connection back home(Amazon) and start parsing out the commands for different devices and passes it along to the smart things*

which takes over from there."

Participants with the advanced model discussed how information flows through the infrastructure as well as to the companies' servers and comes back to the device. These participants personally installed all of their smart home devices. Also, a number of them did some customization in their smart home, i.e., used IFTTT to automate the devices, installed a personal server or built a central assistant using Raspberry Pi. It can be one of the reasons behind their more comprehensive understanding of the network topology. Additionally, these participants are also more informed of the complexity of the flows as well as the fact that devices are sending information to companies' servers as soon as they interact with them.

Participants with the service-oriented model (n=12) have a reasonable understanding about which devices communicate with each other inside the house, but do not have deeper technical knowledge of how that communication happens other than via the WiFi. Their mental models of the smart home mostly consist of the interaction between the smart devices (i.e. lights) and the controller (e.g. Google Home) they use to control the device, but no awareness of the role of other networked components in the device interaction (Figure 1b). There were a few participants in this group who brought up that information is going to the cloud initially when drawing their smart home; the other participants didn't. However, when asked directly during later interview questions they all indicated that information the devices are collecting is not stored locally, it is leaving their home to the cloud or some server. However, the participants with the service-oriented model expressed no or very shallow awareness of the role of the cloud in the device interaction.

3.3.3 End Users Perception of Data Practices

In our analysis, we found that participants' mental models of how their smart home devices work do not often relate to their perceptions of smart home device data collection, usage, and sharing practices. Rather, their understanding is primarily based on interactions they have had with the devices or what they see in the corresponding applications. Some participants ($n = 10$) beliefs of data practices were informed by their perception of particular companies and experiences with those companies in other (non-smart home) contexts, which sometimes leads to inaccurate conclusions on what really happens. For example, Id11 thinks that companies will not sell any data because it would upset their consumers and the companies would lose reputation. Only two explicitly reported privacy policies as a source of their knowledge about data practices. Below we discuss the findings on end users' perceptions of data practices in detail.

3.3.3.1 Data Collection:

Not surprisingly, participants' perception of data collection was informed by the type of the device and their experience with that device. For example, all participants who have a smart doorbell or camera were aware of the device collecting video recordings, but none demonstrated any awareness of the corresponding applications tracking their location whenever they use it. In other words, participants were well aware of the primary data that the device is collecting but may overlook secondary data that does not directly correlate with the type of device or basic utilities received from the device. In Table 2, we summarize user perceptions of what information is

collected for different devices. Only the devices owned by more than five people are listed.

For most of the devices, participants believe that their usage and interaction patterns are being recorded and they were not that concerned about the data collected by the smart home devices. We also looked more specifically at audio and video data since previous studies[92, 71] found that these data are more sensitive to people. When put in practice, video is still considered as the most sensitive; however, participants for the most part were able to find practices that allowed them to be comfortable with the collection of video. For example, using the camera in a live streaming mode without recording the video, starting video recording only when the house is empty, or using an outdoor camera or video doorbell, so nothing inside the house gets recorded. For instance, Id7 mentioned:

"*Only information I would potentially ever be concerned with, like the way I use my device, is the images on the camera. But again, the camera is turned off when I am home, and on when I am not home.*"

However, in one extreme case, a participant (Id22) removed an indoor camera from her apartment. She reported being unable to use the camera outside because of concern of residents of her apartment complex. She was not aware of other alternative configurations for her camera such as using the camera only for live streaming or removing the recordings from the cloud, which she may have been more comfortable with.

Participants did not show much concern about the collection of their audio data. They know that the voice assistant is recording after the trigger word, and they were

comfortable with the audio being recorded in that way. One non-installer participant (Id20) was uncomfortable with the voice assistant as she suspected that Amazon Echo may be listening to her even if she is not calling it using the trigger word. Her Echo had recently showed an Amazon package delivery notification with yellow lights, and she misinterpreted it as the device listening to her conversation. Even though her husband later clarified the misunderstanding, the participant was still very uncomfortable and did not want the device in her house at the time the interview was conducted. Another technical participant decided not to buy any commercially available voice assistants because of a worry over companies harvesting the audio.

Despite their awareness, many participants ($n = 15$) believe smart home devices are collecting more information than they should. However, some participants ($n = 9$) said the data collection was mostly positive. These participants explicitly mentioned that most of the data these devices collect is needed in order to either provide them the services they expect or to make the devices more convenient to use.

We also asked participants what can be inferred about them from the data these devices are collecting. In contrast to a previous study [92], we found that participants are somewhat aware of the sensitive information that can be inferred from the seemingly innocuous data collected by the smart home devices. For instance Id11 mentioned,

"*They can probably tell that I don't have the lights everywhere at my home. That I am out of the house during the day time. They can probably tell when I am sleeping because the lights are not turned on that time.*"

The types of inferred information that were mentioned are: habits and preferences

(i.e. buying habits, music preferences, etc.; 14 participants), daily schedule (i.e. when home or not, when using which devices, etc.; 11 participants), tentative location of the house (8 participants), other occupants in the house (i.e. have pets or kids; 3 participants), political views (2 participants), sleeping patterns (2 participants) and other devices in the house (2 participants). Three explicitly mentioned that these companies can infer a lot of things that consumers can't even imagine.

3.3.3.2 Data Storage:

When prompted, all participants reported being aware that at least some of the smart home device data is being stored externally, with twenty specifically mentioning the cloud or a server operated or owned by the manufacturer of the device. However, three other service-oriented participants expressed a vague idea such as 'somewhere in some kind of database.' For example, Id15 said:

"*I don't know really where it goes or what happened to it but I imagine that it does get stored somewhere, some kind of database and somebody is able to analyze and see different trends through it. But I have no idea.*"

Eleven participants explicitly mentioned there is either no or very limited local storage of the data, that everything is stored in the cloud. Participants frequently mentioned they have no control over the data once they shared it; however, some ($n = 5$) hypothesized that it might be possible to remove their data by contacting the device manufacturers. Interestingly, 4 participants suspected that even if they remove the data, it will still be in the cloud. A number of participants ($n = 8$) also mentioned companies are doing the bare minimum to protect their consumers' data in the server.

Most participants were not sure about companies' data retention practices except for the retention period of the video. Some of them also made interesting inferences, for example, five participants believe that Google and Amazon store data forever or for a very long time because these companies have enough resources to store such data, while smaller companies do not.

Interestingly, all the participants who installed the camera or video doorbell themselves ($n = 7$) know about the video deletion option or after how many days the video will be automatically removed from the server. On the other hand, participants who have not installed ($n = 3$) the camera or the video doorbell are not sure about the storage policy of the video or the option of deleting the video. Video is the one exception where some participants are very aware of the data storage practices and available controls, but only those who installed it, and as a result, they found practices that they were comfortable with and configured their device accordingly. But, participants who are not the installer did not get that understanding, which in one case led to a lot of discomfort and removal of the device.

We did not find as many difference between installers and non-installers regarding their knowledge of data storage policies and controls provided by the devices that collect audio. Out of 20 participants who had a smart voice assistant, 15 are familiar with the device usage log where they can review their voice interactions with the assistant. However, some of them either are not familiar with the data deletion option ($n = 5$) or skeptical that Amazon or Google may keep the data even after they delete it from the log using the available interface ($n = 4$). However, all the participants who did not know about the device usage log were also not involved

in device installation. For one participant, this lack of awareness also lead to more discomfort about using the device, as stated by Id20:

"*I have asked my husband to disconnect the Alexa(Echo) multiple times. Just because I'm not comfortable with it. But if it did collect data, I would have no idea how to find it and to remove it so I would just disconnect it.*"

3.3.3.3 Data Use:

Participants discussed three primary uses of the data their smart devices collect. The most frequently mentioned use case is targeted advertising or marketing to sell products to consumers ($n = 19$). For instance, Id19 said:

"*They have put a lot of money in this product, and then they are selling it. So, they must be using it for something other than me telling my house to turn on my bedroom light. They are building advertising model of me. They want to know who I am and how I work so they can try to sell me something.*"

Participants were aware that their habits, preferences, and daily schedules can be inferred from the data smart devices are collecting and can be used for targeted advertising. However, targeted advertising seems to have became so integral to participants' lives that they accepted it as a price of living in the age of the Internet.

Many ($n = 17$) mentioned that the companies are using the data to improve the current product, for instance by fixing malfunctions/errors (4 participants), improving the user experience or tailoring the device to customers needs (4 participants) or improving the services provided by the device (2 participants). As Id7 stated:

"*(Companies use the information) in order to better the products I guess. I guess*

if there are errors like you know if I ask Google Home to do something, and the lights don't respond, they're surely collecting that kind of information"

A number of participants ($n = 9$) also believe that the information companies are gathering can help them to recognize users' needs and come up with new products.

3.3.3.4 Data Sharing:

Participants identified a number of entities that they believe have access to the data their smart home devices are collecting: the manufacturer of the device/the data analysts working with the company ($n = 23$); third parties/advertisers interested in the data ($n = 9$); parent companies, subsidiaries or affiliates of the device manufacturers ($n = 7$); hackers ($n = 7$); legal organizations such as government security agencies ($n = 4$); the manufacturer of the device/app that is used to control the device ($n = 3$) and other people who have accounts with the device ($n = 2$).

We then asked participants if they think companies share any information with third parties. Twenty-two participants agreed that they do. Nine further believe that companies are sharing only their demographics or preferences but not any personal information; however, 4 participants mentioned they believe companies are sharing everything. Participants also made interesting inferences about how the sharing happens, such as that the big companies (Google, Amazon, Apple) do not share data at all while only the small companies share their consumers' data (6 participants). For example, Id8 said:

"*I think Amazon would be like the top consumer of this information; I think they're collecting this for themselves. I don't think they would share it. I think a smaller*

company... if the Ring wasn't purchased by Amazon, I think Ring might share that information with Amazon...I have a feeling that's why Amazon bought them."

Most of the participants ($n = 18$) said they agreed to this sharing by signing the terms of service or privacy policy or saying 'yes' to everything during the installation process. But similar to previous research[63, 46], participants reported not reading privacy policies and pointed out the usability issues of such agreements. Three service-oriented participants believe they consented just by using the product. Some participants ($n = 9$) stated that once the data is sent to the cloud, it is out of their hands and control. Id12 stated:

"I'm sure they do... absolutely they do it (share data)... they are allowed to do that...they can do whatever they want with it, that data is considered as their property. They can keep everything for their own or they share."

Many participants reported that the only way they can opt out from this sharing is to stop using the product ($n = 15$), while a few mentioned modifying the applications' settings for partial opt-out ($n = 4$) or by contacting the company (n=2).

To summarize participants' perceptions of data practices: they base their understanding of what data is collected on their experiences and interaction with the devices. For the most part, they expect that their data resides in the cloud and that it can be and is shared by companies, with little ability to control that. However, participants expressed a great deal of uncertainty when they discussed the ways companies are collecting, using and sharing their data. The only exception is the video data where all the participants who installed the device were aware of where the video is stored

and video retention time. Several participants ($n = 5$) explicitly expressed their concern about companies not being transparent enough about their data practices. Many participants mentioned that they want more transparency from the device companies ($n = 14$). For instance, Id9 said:

"*If these companies are sharing my data with third parties, I'd like to know who they are sharing with, maybe like if I go to the Insteon website they say, hey we share your data here. So a website that keeps track of all this stuff would be good.*

Participants also want companies to take enough measures to ensure their data is protected ($n = 9$). A few participants ($n = 4$) also believe there are not enough regulations in place and that policymakers should enact and enforce more strict laws to protect consumer data. Finally, ten participants expressed the desire to have explicit control over data collection and sharing and to be able to remove their data from the cloud.

3.3.4 Security and Privacy Threats and Consequences:

We now turn to participants' perceptions of the risks and behaviors for protecting their information. Participants identified several threats and discussed how these affect their security and privacy. However, we again could not find many differences between participants with different technical knowledge levels and mental models. Instead, many of the concerns participants mentioned came from their experiences with the Internet, computers and mobile phones instead of threats specific to smart home devices.

3.3.4.1 Threats:

The most concrete and frequent threat mentioned by participants ($n = 17$) is a data breach in the cloud and their personal information being compromised. Two participants also suggested hackers could gain access to aggregated profile data from the cloud. Id2 stated his concern as:

"*I mean especially the states of data breaches lately. That is concerning because they're not viewing in a way that hey, these are actual consumers out there, these are real people. Then they may not have the best security practices, and that data can get out somewhere.*"

Some participants ($n = 11$) also pointed out that their smart home devices or the WiFi can be hacked and remotely controlled by adversaries for various reasons, i.e. to spy on them, break into their house, etc. For example, Id19 said:

"*someone could access my lights, someone could turn my heat up ... umm ... if I had a smart lock, someone could have access that to get in my house but I don't have a smart lock. Just like I wouldn't use banking through any of these devices because the consequences are too severe in case there was a breach... the same with a lock, I wouldn't use one of those.*"

Six participants also identified improper use and sharing of their data with third party companies as a potential threat. Unlike data breaches and device hacking, participants were more vague about this threat, i.e., third party companies may use my data for some nefarious reasons or their server may not be secure, etc. Id12 said:

"*The person you shared that data with can share the data with somebody else. Like*

if you shared data with the company that follows all the rules and if they share with a company that doesn't follow any rule that is out there. I don't think these companies have any methodologies in place to ensure that whether their partner will maintain the data safety or not."

3.3.4.2 Consequences of the threats:

These threats were then associated with specific negative outcomes. Similar to the concerns expressed in previous papers on smart homes [93, 88], participants most frequently mentioned the violation of their physical security and safety ($n = 10$). They implied that smart home devices know when they are home or not, and what other devices they have in their home, and that this information can be used to rob them or physically harm them. Id3 mentioned:

"*I guess if it was a criminal group like a gang or something they could use that data to know when I'm home or not home. If they want to rob, what is the best time to rob, where to go in my house, what my house looks like, that kind of information.*"

Participants also mentioned the possibilities of identity or financial theft ($n = 4$). Three advanced participants expressed their discomfort about the abilities of companies to manipulate their decisions, judgment or perception of things in some way. Id23 said: "*I think they can show me what I like; I think they can alter the world I am living into the world that is preferential to me, as a consumer.*"

Other risks that participants identified are profiling (n=2), criminals/companies using data to uniquely identify people (n=2), spear phishing (n=1) and social engineering (n=1).

Interestingly, some participants ($n = 6$) shared a general discomfort around the feeling of surveillance, of people knowing too much information about them and being able to use that for nefarious reasons specially around the devices that collect audio and video. For instance Id20 mentioned:

"*Makes me feel uncomfortable that I am in my own home and I can't just say whatever I want without somebody listening you know?*"

Participants with the advanced model identified more examples of threats, and 8 of the 9 were concerned with data breaches. However we found no additional differences between participants based on their mental models. In line with the previous work [88], we found that despite participants identification of these threats, only a few expressed significant concerns or worry about them. However, participants did take some actions to protect the security and privacy of their smart home as we will further discuss below.

3.3.5 Protective Measures

Participants reported a diverse range of protective measures that they perform or are aware of to reduce their security and privacy risks. Both traditional security best practices and use of protection tools/services were discussed by participants.

3.3.5.1 Behavioral/non-technical mitigations

Many participants ($n = 12$) mentioned self-censoring their way of using smart home devices. It took various forms, such as turning the device off, changing behavior in front of the device, or avoiding the use of certain device functionality ($n = 6$), as well as limiting the amount of information disclosed to the device ($n = 8$) by not providing

more information than absolutely necessary while signing up for an account, or by using someone else's account. For instance, Id22 mentioned changing her behavior in front of the camera:

"*It knew when I woke up and walked to the kitchen... it is in the living room... so it kind of sees that I come around the corner to the kitchen...I kind of try to stay by the wall because I didn't want my robe or pajamas or whatever I was wearing to be on camera.*"

Some participants ($n = 8$) also expressed concerns about their financial information and mentioned frequently monitoring their bank accounts and using credit monitoring services.

3.3.5.2 Technical mitigations:

Participants discussed using various traditional technical security practices ($n = 9$), such as changing and using strong passwords and using two-factor authentication. Two also reported using certain devices offline to limit access to their data. Two participants with the advanced model also discussed using a separate network for smart home devices. Id8 stated:

"*I have a closed WiFi network for my IoT devices. I do password changes and what not, also my WiFi isn't broadcasted.*"

3.3.5.3 Tool-based mitigations:

Participants also discussed using some tools or services to protect their privacy around smart home devices ($n = 7$). Two participants hosted local servers and customized the devices to work with that. Others mentioned using different network

security devices, installing firewalls or a VPN to protect their network from outside attacks. Id3 stated:

"*I do have a firewall set up on my network that apparently helps with if people try to get the data from me... I can't do anything about the data stored on the cloud. Hopefully the firewall cuts down on any devices that might be compromised or part of a botnet or something like that.*"

A number of participants ($n = 5$) expressed their awareness of such tools or services but were not using those at the time the interview was conducted.

The tool-based mitigations were primarily discussed by the more technically knowledgeable users; nine of the twelve who mentioned tool-based mitigations had the advanced mental model. Furthermore, only the participants with advanced mental models demonstrated familiarity with customizable tools/services for preventing their data from being sent out to the Internet ($n = 5$). On the contrary, most of the participants with the service-oriented model attempt to mitigate their concerns by following traditional security practices (e.g. changing passwords) derived from other computing contexts or changing their behaviors around the devices.

In summary, participants have demonstrated an understanding of some risks from the smart home, but they are not very concerned about many of them. Only a few technical participants did use tools specifically to protect their smart home. Others kept on following the best practices they know from other contexts either because they don't know about what actions to take in the smart home context or the cost of finding and taking those actions is way bigger than their concern. Participants discussed a number of reasons for their lack of concern and unwillingness to take

protective measures, as discussed in the next section.

3.3.6 Reasons for lack of concern and protective actions

While participants could all discuss perceived threats to their security and privacy, most did not express strong concerns. Several themes emerged when we asked participants why they are not concerned about their security and privacy in the smart home.

Acceptance of trade-off: Most of the participants (n=15) mentioned that they have to give up some of their data and accept the risks for the convenience and services provided by these smart home devices. Four participants also mentioned feeling powerless over this trade-off. For instance, Id12 said:

"*Once I bought all these devices that was it. These functions come with these risks no matter what and I can't do anything about that. There are no third option. If you want the device you have to accept those risks, otherwise don't use it at all.*"

Though participants accepted the trade-off between their privacy and the convenience, 13 of them stated a desire for more transparency from the device manufacturers.

Trust of the manufacturers: Another common reason was participants' trust in the device manufacturers. Eleven participants stated that they trust that companies will not misuse their data because it would damage the company's reputation or will not be financially profitable. Id7 said,

"*I don't think they (companies) are selling it to Russian, I don't think they are*

trying to steal my identity. I don't think there's anything other than just trying to improve the product, trying to use the information for marketing and advertising."

Optimism bias: A number of participants ($n = 9$) expressed a low likelihood of being affected under the assumption that they are not an attractive target for hackers. For instance, Id10 mentioned: "*I also went to college and have student debt. So, I don't feel like an attractive target for someone to try to steal my identity or really do anything.*

Marginal risk: Participants tend to judge the risk from smart home devices by comparing it with how exposed they already are. Several participants ($n = 9$) were not concerned because they believe a wide array of information about them has already been collected or available otherwise and the smart device won't increase the risk. For instance, Id13 said:

"*I've been using the Internet since like I was in middle school... so I don't really have an expectation of privacy.*"

Ten participants believe the data that smart devices are collecting are not that useful or sensitive and would not be harmful to them in the future. Five participants also explicitly mentioned not being concerned because smart devices do not have any critical information about them, i.e., financial details, SSN, etc. Id16 mentioned:

"*I would be worried about just the things like my credit card information or maybe like social security... that hasn't been shared with any other companies... as for like my habit I don't really think that's (concerning) because the companies will only be*

able to tailor the things we want."

Three of these participants also felt that they have already taken enough action to keep their smart home safe.

Trust of regulators: Four participants believe that there are appropriate regulations or overseeing bodies in place which will protect their data from potential misuse by companies. Id19 said: "*If they(company) violate it(rules) it's either going to be corrected or will be most likely to be shut down by a government agency or something.*"

High cost of protective actions: A few participants (n=3) with the advanced mental model also discussed the inconvenience of implementing useful protective measures. For example, Id9 explained the inconvenience of locally hosting the services:

"*You know if I wanted some services that did not connect to the Internet then I kind of have to purchase that myself and run everything that way to prevent, you know, things on my network from going out to the Internet.*"

3.4 Discussion

We will now report the key insights learned from our study and discuss implications and recommendations for designers, policy makers and researchers.

Knowledge of smart home does not influence threat model or trigger actions: Even though participants had different levels of understanding about how their smart home works, their perception of device manufacturers' data practices was

quite similar and not much different from the findings of the earlier work on Internet perceptions [45]. Furthermore, our participants' knowledge about their smart home and manufacturers' data practices did not affect their awareness of possible threats in the smart home. Rather, participants with advanced and simple mental models both frequently mentioned threats and protective actions that are known from the context of the Internet, but also applicable in the smart home. However, participants with the more advanced mental model did show more awareness of the protective measures unique to the smart home, such as preventing data from going outside of the home. Yet, despite awareness of the threats and protective measures, most of the participants choose not to put those into practice. Instead, participants' decisions of protective actions were more influenced by their own biases and concerns related to general Internet usage.

Difference in knowledge (or a lack thereof) between different participant groups: The two groups that emerged in our analysis, i.e., participants with the advanced and service-oriented model, seem to differ primarily in their technical detail and understanding of their smart home. While the participants with advanced model were all installers, there were installers with the service-oriented model as well. However, we did not find many differences between participants with these two mental models and installers vs. non-installers in terms of their perceptions of data practices. The only difference in knowledge is that the installers of smart cameras and doorbells are more aware of companies' video data storage practices. One reason for installers having this awareness can be the fact that the users need to buy an addi-

tional subscription to store the video in the cloud for many of the devices (i.e., nest aware subscription for nest camera, ring protect plan for ring doorbell). This added step exposed the installers to the company's policy regarding video data storage.

Users' lack of exposure to companies' data related policies, in general, may be the reason for the similar perceptions of different groups of participants. This asserts the need for including such information about data practices as a part of the application that is used to control the device and designing nudges and cues for users (installers and non-installers) to get exposed to that information.

Trust paradox: Participants know about much of the data collection occurring with their smart home devices. Many of them are also aware of companies' lack of security in the cloud and data sharing with third-party organizations. Some of them also believe that there is not enough legal protections for consumers. Yet, participants justified their lack of concerns and protective actions with trust that companies will not misuse their data as it will tear down their reputation and regulators will close the company. This paradox can be explained by the notion of learned helplessness seen in many participants, where they ignored possible negative consequences because they feel they have no control. Participants described how once data is collected from their devices, it's beyond their control. And sometimes coped by censoring themselves in some way to keep data from being captured by a device and entered into an application in the first place. Participants thus primarily rely on the organization to keep their data secure and expect governments and policymakers to regulate what is occurring, rather than taking many actions by themselves.

Estimated risk is too low to take action: One of the main reasons for inaction is that participant's estimated risk from the smart home devices is quite low. They are aware of the fact that their daily schedule and habits can be inferred from the data smart home devices are collecting and that companies may use that for targeted advertising. However, companies have been using data such as buying habits for targeted advertising for a long time; it was nothing new to the participants and not viewed as an added risk. Even the risk of a break-in was also not able to raise participants' concerns as they believed they would not be a potential target. A number of participants also didn't think that the use of smart home devices may increase their risk of identity theft as they think there is already enough information out there on the Internet if someone wants to target them specifically. Even the participants who have been a victim of identity theft were quite comfortable with their smart devices as they believe they put enough protection on their financial accounts. None of the participants showed awareness about news of potential smart home device or data misuse, and may not realize the breadth of risk imposed by their devices. Rather, all the participants accepted the trade-off between the benefit of smart home devices with their lower perceived risk as mentioned by Id19, "*I wouldn't let something that I personally see so small affect something that I am enjoying using so much. Something that I personally think more serious, like access to my bank and things like that.. I would lock it down and stop using it immediately.*"

Lack of awareness about data practices and controls impede usage: De-

spite participants' perceptions and expectations of a large amount of data collection and sharing, we also note that participants are still very uncertain about the device manufacturers' data practices, echoing prior work on users' perception of the Internet and cloud storage more generally [45, 17, 27]. Many participants were also uncertain or unaware of the controls they have on their devices. For a few participants, these uncertainties led to not using certain device functionalities or using the device only at specific times or specific places and may also influence their freedom of expression. In two extreme cases of non-installer participants, Id20 and Id22, it led to the desire of removing the device from their house. However, from their interviews, it appeared the awareness of the available controls may have influenced their privacy behaviors, as mentioned by Id22, "*If I had an easy way to do it... if I had to push a button to remove it(camera recordings) then I would surely remove it.*" In other words, more familiarity with controls may have led those participants to be more comfortable using the device. This underscores the importance of future research to examine ways to nudge users, especially those who are not involved in the set-up and configuration of their smart home, to discover and utilize the available controls.

3.4.1 Implications and Recommendations

Enhance transparency and control: People want more transparency and control over the data collected and shared by smart home device manufacturers. Participants should have the ability to remove the data and set sharing preferences of their data where possible, for instance, sharing only aggregated data, sharing only usage data, etc. Companies can provide more transparency and controls to users by designing

a dedicated web-page or privacy setting in the mobile application where users can view the data points collected by the devices. Another suggestion is to provide privacy and data-related information in addition to the set-up information in the box, which as Peppet[73] reported, many of the IoT device manufacturers do not. Multiple participants appreciated Google for the transparency and added control in their devices, whereas some were more skeptical about buying devices from lesser-known companies. New smart home start-ups can improve their reputation by providing more transparency and control over users' data.

Researchers have also proposed and developed dedicated devices and tools to give users more security and privacy controls[11, 78, 79]. For instance, Karmann et al. developed 'Alias,' a device that paralyzes the voice assistant by preventing it from listening and only activates the assistant for a custom wake word from the user[11]. Mennicken et al. proposed a calendar-based interface, Casalendar, that visualizes triggered actions and the sensor data collected in a smart home to facilitate users' understanding [68]. We advocate for more such research on novel security and privacy tools and controls beyond the features currently available within a device. While few of our participants were actively looking for additional tools, we believe that easy to use off-the-shelf tools, if commercially available, may increase the comfort of privacy-sensitive people and provide more options for privacy preserving use and adoption.

Best practices for companies and users: As smart home devices become more widespread, smart home attacks will also become more common. Yet, participants who have simpler mental models of their smart home are often aware of and adopted

only common traditional best practices (i.e. changing passwords) that may not always help against the security and privacy risks unique to the smart home. Current measures that can help (i.e. locally hosted services) are too technical for the vast majority of potential users. Yet, it is also unclear what best practices are - what are the best methods for average consumers to protect themselves, their data, and their homes? Thus, we concur with Zeng et al. [88] that security researchers, policy makers, and manufacturers need to develop an additional set of best practices for smart home users. However, we want to emphasize that such best practices should be developed by keeping the mental models of users and their technical capabilities in mind. Our findings also revealed that participantPris rely on companies and policy makers to protect their data. With the widespread use of multiple smart home devices, it will be burdensome for users to manage and take responsibility for all of the data collected and shared by smart home devices. Our study also reinforces the need for the enforcement of a set of privacy best practices for smart home device manufacturers [92]. Policymakers should consider how to administer these rules and penalize companies that do not comply with regulations.

Develop mechanisms to increase user awareness about visual indicators and controls: Researchers need to explore how additional awareness mechanisms can be incorporated directly into smart home devices and applications. For instance, exploring ways to nudge users toward available controls or designing observable cues that provide added awareness of data collection and sharing. For example, Amazon Echo shows blue light patterns when it starts listening. However, designers need to

be careful while designing visual indicators, as we found that use of similar indicators (i.e., showing yellow light patterns as a delivery notification by Echo) can be confusing to users. In addition to developing visual indicators, designers should also explore ways to inform users, especially non-installers, of those indicators as a primary part of interaction with the device. For instance, on the first interaction with new users, the voice assistant can speak out loud about the controls they have over their data.

Educate people about future risk: Most of the recent news on IoT misuse is about the use of devices for Distributed Daniel of Service attacks. People do not feel personally targeted when they learn about such generalized attacks. Furthermore, even though participants were aware of the sensitive information that can be inferred from their smart home data, they were unaware of how that data can be used other than for advertising. Centralized online resources are needed where people will be able to learn about the data practices and possible risks from different smart home devices, so that existing users can asses their risk, and potential buyers can decide whether and which device to buy. Mozilla already provides one such online guide [10], however none of our participants mentioned it. Strategies should be taken to educate users about possible risks and available public resources to find information about their devices.

3.5 Conclusions

In this qualitative interview study of smart home users, we found that participants generally understand that a wide range of information is being collected about their

interactions with smart home devices, and shared with a variety of entities to provide useful functionality as well as for marketing and advertising. Much of this information is stored in the cloud, where it is out of the control of users. Yet users are also highly uncertain about these data practices, and desire greater awareness and control over what is occurring. Participants also identified several threats common across computing contexts - such as breaches and financial theft, as well as home safety and security. Yet, despite this awareness of potential threats, they did not view these as serious risks and practiced few mitigation strategies beyond trying to provide devices with no more information than necessary. These findings provide new information about how users perceive what is occurring in the smart home and suggest the need for greater awareness and user friendly control mechanisms as well as cues and visual indicators to inform and contribute to users' security and privacy practices in their homes.

CHAPTER 4: EXPLORING END USERS SMART DEVICE SHARING BEHAVIOR BEYOND THE HOME

The results from this study have been accepted in the Conference on Human Factors in Computing Systems (CHI), 2020 in Hawaii, USA.

4.1 Introduction

Remote access to a smart home is one of the primary benefits of the smart home devices, where users can check up on and control their homes when they are away. Similarly, we believe homeowners may wish to share this responsibility with other people, not just those who live with them. There are many uses we can envision. Neighbors could check on a home in case of a fire or burglar alarm. Neighbors may also want to share access to each other's security or doorbell cameras to monitor community safety and security [75, 23].

As I have discussed in chapter 2, there is still limited research examining how smart home devices can be used and shared amongst this community of people. I aim to address this gap by focusing on remote usage of smart home devices in particular with the secondary stakeholders: people who do not live in the home. I have conducted a survey and interview study, focusing on the decisions of device owners who may be interested in remotely sharing their smart home devices with people who do not live with them. Our research questions include:

- RQ1: Are smart home users interested in sharing their devices with people who

do not live with them? If so, with whom?

- RQ2: What devices and capabilities do smart home users want to share with people who do not live with them?
- RQ3: For what purpose are smart home users interested in sharing their devices with people who do not live with them?
- RQ4: For smart home users who already share their devices with people who do not live with them, what are their experiences and unmet needs for sharing?

Our results provide detailed information regarding who, what, and why these devices are shared and what are the sharing behaviors, and needs of the users who currently share their smart home devices beyond their home.

4.2 Methods

We utilized two complementary methods to examine smart home users' current and potential device sharing: an online survey and a follow-up interview with a subset of participants. Each method is described in detail below. Participants were primarily recruited using a Qualtrics panel, resulting in 156 online surveys. Of those, six participants who already share their smart home devices agreed to participate in a follow-up interview. To recruit additional interview participants, we advertised on social media and online IoT related forums. Seven additional participants were interviewed, also taking the online survey prior to the interview. In total, we have 163 survey responses and 13 interview participants. All methods were approved by our university IRBs.

4.2.1 Online survey study

We recruited participants who are at least 18 years old, live in the United States, and own at least two smart home devices from the list of devices we presented, including smart speakers, smart home security devices, internet enabled appliances, and other categories of commonly used devices. To assure data quality, we first asked participants a question about the purpose of the study, and screened out the subjects who answered incorrectly. We then asked participants to list up to three people who do not live in their house, and with whom they currently share or would be willing to share their smart home devices. Participants were asked to provide their relationship with each of those people, as well as the proximity of that person to the location where they currently reside.

For each person a participant listed, we then randomly selected three of the smart home devices they own and asked them to choose which kinds of capabilities of those devices that they currently share, or would like to share, with that person. For example, for a smart burglar alarm such as ADT, Nest, or Ring Alarm, users were asked to select from the following capabilities: get a notification when the alarm triggers, remotely arm/disarm the alarm, view the status of the alarm (armed/disarmed), view log information about the alarm, configure the alarm, add new users, install the latest software updates, or other (fill in the blank). Participants were then asked to explain the reason behind sharing their devices with that person, and what benefit they receive or expect to receive from such sharing in a free text response. For any desired sharing, participants were also asked why they do not currently share in another free

text response.

Participants who did not list any people that currently share or foresee sharing with were asked to explain the reason behind their decision in a free text response. Additionally, we asked these participants to explain scenarios in which they could envision changing their initial decision. Finally, we asked all of our participants whether they want other people to share their smart home devices with them and their reason behind that in a free text response. At the end of the survey, we asked participants various demographic questions. On average, it took participants 12 minutes to complete the survey.

4.2.2 Follow up interview study

We invited participants who currently share one or more of their smart home devices with people who live outside of their house to share additional details about this type of sharing. Researchers contacted the participants through email to schedule a semi-structured phone interview. The interviews were recorded via Google Voice and transcribed by a transcription service. On average, interviews lasted 30 minutes per participant. The participants recruited from the Qualtrics panel pool were compensated with a $10 amazon gift card. The participants recruited via forum advertisement were compensated with a $12 Amazon gift card for both participating in the interview and taking the online survey.

We asked interviewees to tell us with whom they share their smart home devices, which devices they share, and for how long they have been sharing those devices. For each device they shared, we then asked participants to discuss the process of sharing

- what they remember of how they enabled sharing, and whether they were satisfied with the controls they have over sharing the device.

We then focused on participants' motivations behind sharing their smart home devices with people who live outside of their house. The participants were prompted to discuss the events that led them to such sharing and why they decided to share with that particular person. We asked the participant to discuss in detail the reasons behind sharing the device and the benefits they received or expect to receive by this sharing.

Next, we focused on participants' perceptions and concerns about the capabilities they shared. We asked them how the people they currently share IoT devices with use the devices, as well as what access and controls the person has. We also asked participants about any concerns they may have around the sharing. Participants were then asked about whether they would want any additional control over sharing their smart home devices, how those controls would be beneficial for them, and whether more control would likely influence their device sharing decisions.

Finally, we asked participants about reciprocal sharing - whether they would want the people they mentioned to share their smart home devices with them. Participants were then directed to discuss the sharing process and the motivation behind the reciprocal sharing.

4.2.3 Data Analysis

Our survey participants' responses included both multiple-choice responses and free-text responses. One researcher performed open coding of the free-text responses

and developed initial codebooks for each, classifying the reasons for sharing or not sharing devices. Two researchers then used the codebooks to independently assign codes to the open-ended survey responses. The Kupper and Hafner inter-rater agreement was, on average, 78.95% (min=74.48%, max=84.48%). The researchers then discussed and resolved the disagreements.

Many of our results are descriptive statistics of our quantitative data, as our survey was not designed to determine statistical significance among different variables. We did use a mixed model linear and logistic regression with random intercept per participant to analyze the relationship between participants sharing behaviors (how many devices shared, what type of device shared, etc.) across different independent variables, such as, groups of people the device is shared with, etc., where reasonable. However, we did not find any statistically significant results for our participant sample.

We used an inductive coding process to analyze our interview data. Two researchers independently coded the interviews of three participants and identified common themes. The researchers then discussed and merged the themes and came up with one shared codebook with 7 structural codes divided into 44 subcodes. The rest of the interviews were then independently coded by the two researchers using that codebook. The researchers kept track of the disagreements, and the inter-coder agreement was measured at 80.6%. The researchers then discussed and resolved the disagreements. We note that our sample size is small, and our interview data is qualitative. Hence any numbers reported in our interview results are merely to indicate the prevalence of a particular theme across our sample of participants.

4.3 Survey Results

In this section, we present the result of our survey study. We start by providing an overview of our participants, then present the details of their current and desired sharing decisions, followed by the reasons behind and the factors affecting those decisions.

4.3.1 Descriptive characteristics of survey participants

The online survey was completed by 163 participants. On average, participants were 45.8 (std. dev.=16.4) years old. 55.8% of the participants were female, and 44.2% were male. Our participant sample was well-educated; 58.9% attended college and have a degree. The majority of our participants live in a single-family home (86.5%), while others live in an apartment (11.7%). 68.1% of our participants own the places where they live and 28.2% rent.

4.3.2 Willingness to share access of smart devices

We were expecting only small numbers of people to currently remotely share devices with people who do not live with them. Yet, almost half of our survey participants (n=78, 47.8%) reported that they currently share their smart home devices with people outside of their homes. Another 16.6% (n=27) do not currently share but want to share their smart home devices with people who do not live in their houses in the future. The rest of the participants (n=58, 35.6%) do not currently share or desire to share their smart home devices with anyone other than the people they live with.

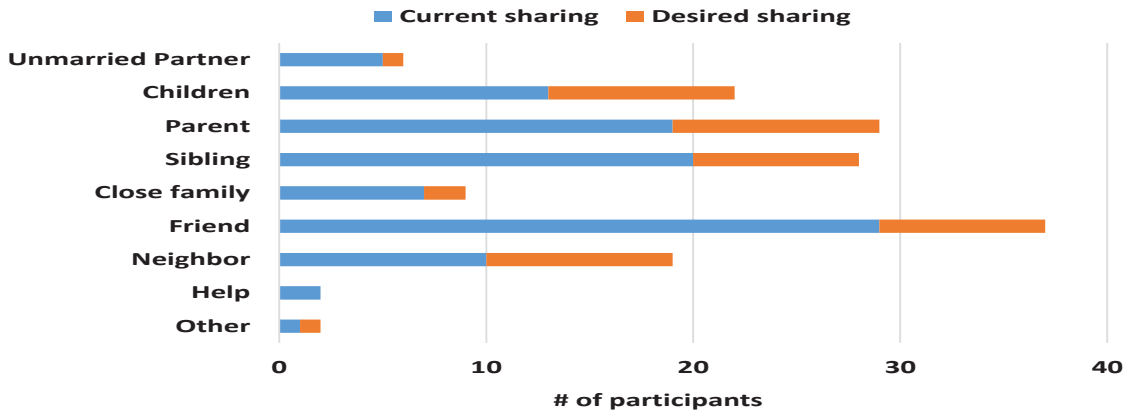


Figure 2: Who do participants share their devices with?

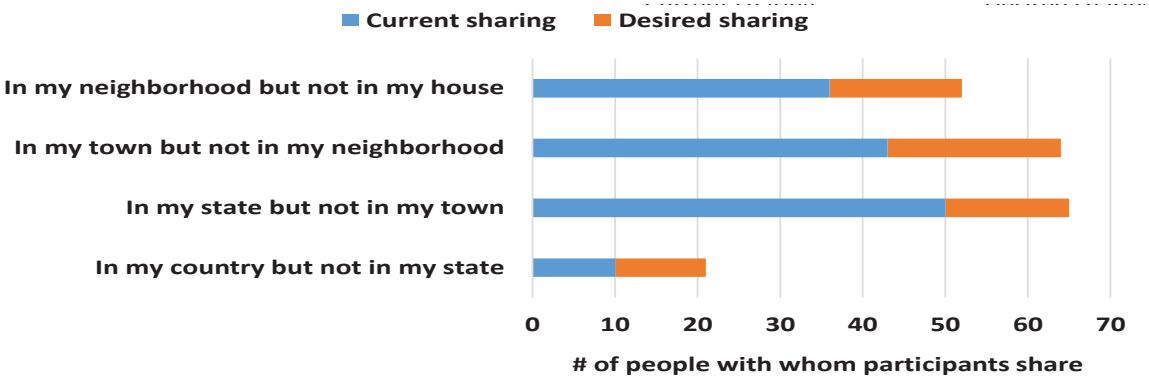


Figure 3: Where do the people live?

To characterize the community with whom our participants consider sharing their smart home devices, we asked what is their relationship with each of the people they mentioned in the survey. Eight relationships emerged from the 202 different people our participants listed: unmarried partner (mentioned 6 times), parent (32 times), sibling (56 times), children (31 times), other close family members (10 times), friends (43 times), neighbors (21 times), and house help (2 times). Out of 105 participants who currently share or desire to share their devices, 83.8% share with a family member, 35.2% share with friends, and 18.1% share with their neighbors (Fig.2).

We then asked our participants where the person they currently share or want to share their device with lives, to examine if the location plays a role in participants' device sharing decisions (Fig. 3). Location does not appear to have much influence, other than for those who are furthest away. Only 14 of our survey participants want to share with someone who does not live in their state.

4.3.3 Devices and capabilities shared

Our participants currently share and want to share a wide range of devices from smart security devices to household appliances with people who live outside of their houses (Figure 4). The most common devices are smart locks (shared by 77.8% of the participants who own the device), followed by burglar alarms (75.8% of participants), and smart doorbells (72.5% of the participants). Smart indoor (61.39% of the participants)) and outdoor cameras (68.8% of the participants) are also frequently mentioned by our participants. Interestingly, many participants shared or want to share the remote access of their smart speaker (60.7% of the participants) and smart

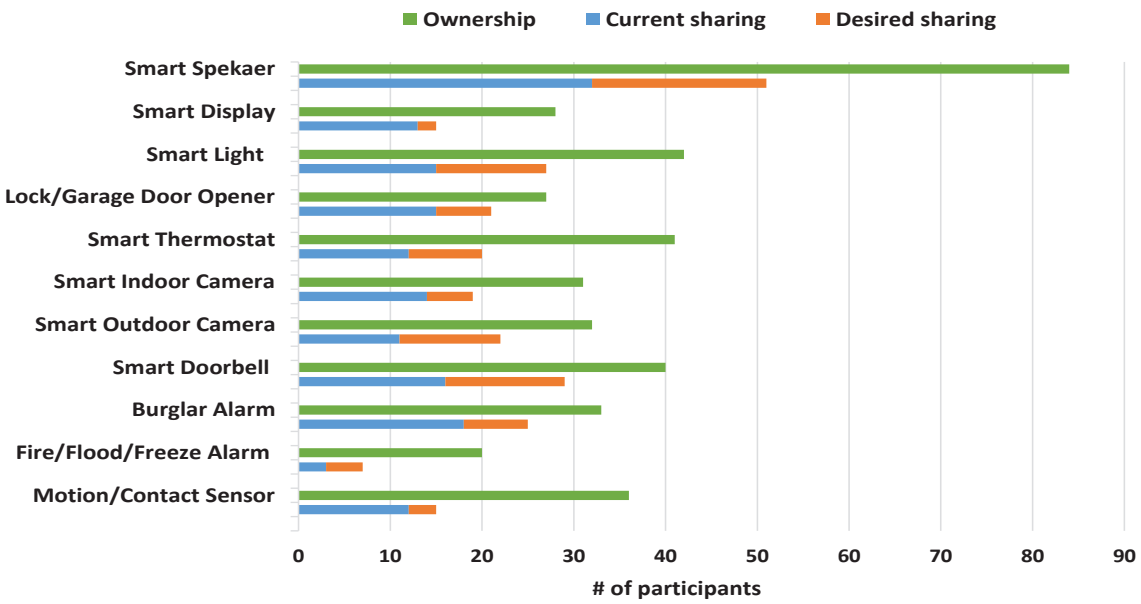


Figure 4: Which devices do participants share outside of the home?

lights (64.3% of the participants) as well, for various reasons we will discuss in the next sections.

To characterize what particular capabilities participants share or want to share for their smart home devices, we asked our survey participants: "Please indicate how your 'PERSON' currently accesses or you want him/her to access the 'DEVICE' from outside of your house" 5. We ask this question for at most three devices for each person the participant mentioned [1]. Hence, the percentages of people for each shared capability was calculated using the total number of people who were asked this question for each particular device, not out of the total number of people with whom participants currently or want to share the device. Details for 4 devices are shown in Figure 5.

We found that for smart cameras and doorbell, the most frequently shared capa-

[1]Devices were selected randomly from the list of devices participants currently share or want to share if there were more than three.

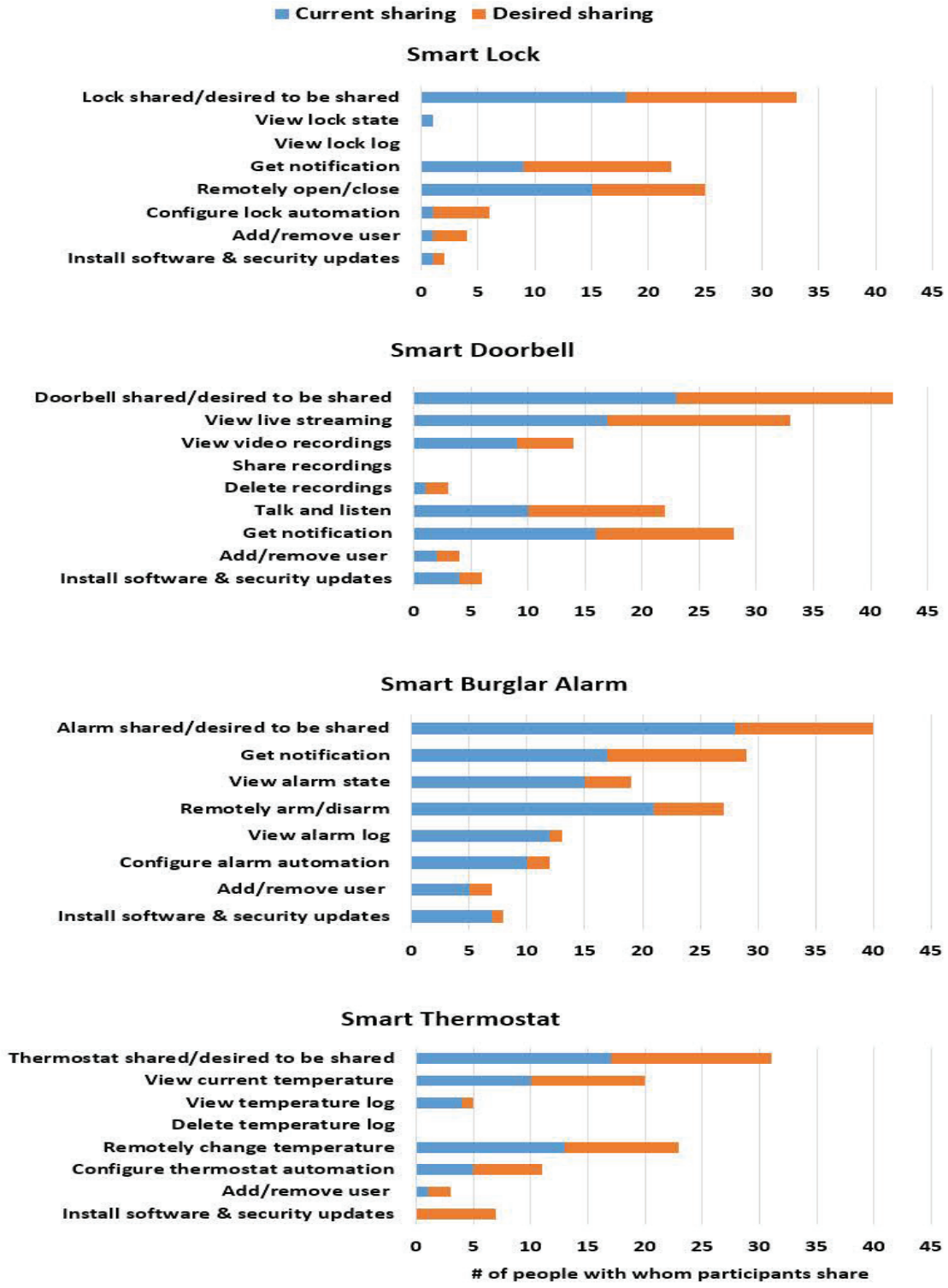


Figure 5: Which capabilities do participants share?

bilities are viewing live streaming (shared with 77.4% people for the indoor camera, 81.3% for the outdoor camera and 78.6% for the doorbell), followed by receiving notifications of motion and rings. Not surprisingly, receiving notifications was the most shared capability for the smart burglar (with 72.5% of people) and fire/freeze alarms (with 80% of people) and motion/contact sensors (with 80% people).

Our participants mostly shared or wanted to share the remote control access for smart appliances (shared with 83.3% people for smart light and, 74.2% people for smart thermostat) and smart speakers (with 58.7% of people). Interestingly, the 'Drop In' capability was shared or desired to be with 42.7% of the people with whom participants share their smart speaker. This feature allows the permitted users to begin an audio call anytime without the need of the receiving party picking up the call. Users rarely chose configuration capabilities, such as adding users or installing updates, for their devices. Although, almost all capabilities were still chosen by a small number of participants.

4.3.4 Reciprocal sharing

To learn more about how smart homeowners perceive the device sharing relationship among people in the community, we investigated our participants' preferences on reciprocal sharing: do the participants want people outside of their homes to share smart home devices with them? Participants who do not envision sharing smart home devices were similarly pessimistic towards someone else sharing devices with them. Only seven participants reported that they would be interested in such sharing [2].

[2]The question about reciprocal sharing was only shown to 40 out of 58 of those participants.

However, participants who do consider sharing their smart home devices with people outside of their homes were more open to reciprocal device sharing. Many of these participants (n=61, 58.1%) reported reciprocity in device sharing activities at present or showed their willingness to do so. These participants currently have access or want access to the smart devices of 54% of the people they listed in the survey.

4.3.5 Reasons for sharing (or not) devices beyond the home

Our participants provided a range of reasons for both sharing and not sharing their smart home devices and related capabilities with people outside of their homes. These reasons also shed light on the benefits participants receive from sharing those devices and the concerns that refrain others from sharing. From coding all the open ended responses, we identified three main factors affecting participants' smart home device sharing decisions [3].

Benefits received from sharing the devices

The perceived benefit was the driving factor for sharing smart home devices with people outside of the home, mentioned by ninety-five (58.28%) of our participants. Slightly more than half of the participants who stated a benefit as a reason for sharing (n=53,55.8%) said that they share or would share their devices to increase the security and safety of their house. They mentioned that the person they share the device with could monitor their house and delivered packages in their absence, get notified about any emergencies and take appropriate actions. For instance, id77 said:

"When an emergency occurs at the home (attempted break-in, fire, etc), an indi-

[3]Please note that the numbers presented for each of the factors represent both wanted (or unwanted) sharing and reciprocal sharing.

vidual outside-of-the-home receiving the notification from a smart device that such an event is happening could lead to extra security, if the friend is closer to the home than residents at the time or (when resident) cannot respond from inside the home due to safety concerns."

Another commonly stated reason for sharing was providing easy access to the devices and home from both inside and outside of the home, mentioned by 53.6% (n=51) of the participants. This took various forms. For instance, the smart doorbell was shared so that the person can remotely talk to visitors at the door, while the smart lock was shared so that the person can let themselves or other people in, especially in case of emergency or in the absence of the owner. Other devices, such as burglar alarms and lights were shared so that the person can remotely turn them off if they are accidentally on or use the devices when they come to the house. For instance, id155 justified sharing his lock and lights with a friend:

"Peace of mind that she has access in the event something happens to myself or my spouse, and also when she visits the access works when she's in the home as well."

Finally, a number of participants (n=32, 33.7%) mentioned sharing smart devices that would help to easily monitor the safety of the pets and people in the home. For example, id105 said: *"They (parents) are getting older and in worse health, and it would make me feel better to have 24-hour access to them."*

Ten of these participants also mentioned that smart home devices are another method of communicating (i.e., the drop-in feature of the smart speaker) with friends and family.

On the other hand, sixty (26.8%) of our participants mentioned not sharing at least one device or capability because they felt it is not necessary at that particular moment, there was no perceived benefit. However, 14 participants (23.3%) stated that they would share the device or the particular access with people outside of the home if the need arises, for instance, in case of an emergency or when they go on a vacation. For instance, id105 mentioned: *"I'll share if my children or anyone was home alone and in bad health or needing emergency services."*

Security & privacy of the house and inhabitants

Security and privacy-related reasons were stated by fifty-three (32.5%) of our participants to explain why they do not share some or all of their devices with people outside of their house. These participants frequently mentioned that sharing smart home devices or particular capabilities would make them uncomfortable and increase the chances of security and privacy attacks (both physical and remote), jeopardizing the safety of the people who live in the house. Participant id144 mentioned:

"I would be afraid to have my information get into the wrong hands, robberies take place, and people that are not supposed to have access will, and it just seems like it would cause big problems. It makes my environment accessible to negativity."

Some of these participants (n=23) also mentioned avoiding access to anyone else's device because they do not want to intrude on others' private spaces or have the liability of managing their devices: *"I just don't want anyone's information. I don't want to accused of something I didn't do"* (id97)

Traits of sharing partners

Another factor that participants consider during sharing is the characteristics of the people they want to share their device with. Eight of the participants mentioned sharing with someone who is knowledgeable about the smart home devices and would help with the installation or maintenance of their smart home. For instance, id66 stated:

" My brother is an IT security analyst. I have him basically manage the update, and upkeep of my smart home devices. It's very convenient whenever I would forget to do it myself. He also tells me whenever someone connects to my devices, and to adjust my password and whatever else when necessary."

On the other hand, 12 participants mentioned that they do not share their devices because of some difficulties related to the person with whom they want to share the device. For example, the person is busy and could not meet to discuss the sharing; the person does not have a smartphone or is not knowledgeable enough to manage the device. For instance, id156 said: *"The Ring(alarm) will auto-disarm if he inputs his password, but he still is not very tech-forward and calls me prior to dropping my house to ask, "is the house armed?" On the flip side, I'm not sure how he would be notified the alarm was off if he is using a flip-phone."*

The proximity of the the people to the home (mentioned by 2 participants) and the level of trust participants have with them (mentioned by 24 participants) also affected sharing decisions. Ten participants share their smart home devices because they trust that person explicitly, while 14 others mentioned they do not have a person

ID	Gender	Age	Devices currently shared	With whom currently shared?
Abby	F	31	Smart Doorbell	Parent
Lucia	F	38	Smart Speaker, Display, Thermostat, Indoor Camera	Parent, Sibling
Travis	M	21	Smart Speaker	Sibling, Close Family
Jim	M	67	Smart Doorbell, Burglar Alarm	Children
Eric	M	37	Smart light, Lock/Garage Door Opener, Fire/Flood/Freeze Alarm	Close friend, Parent, Sibling
Amber	F	39	Smart Lock/Garage Door Opener, Indoor Camera	Parent, Close Friend, Pet-sitter
Matt	M	29	Smart Indoor Camera	Sibling, Close Friend
Daniel	M	26	Smart Light, Thermostat, Lock/Garage Door Opener	Close Friend, Parent
Max	M	39	Smart Indoor Camera	Parent, Siblings
Ben	M	41	Smart Speaker, Light, Lock/Garage Door Opener, Indoor Camera, Burglar Alarm	Girlfriend, Parent
Mark	M	26	Smart Speaker, Doorbell	Sibling
Joe	M	48	Smart Speaker, Light	Children, Roommates Family
Violet	F	39	Smart Doorbell	Close family

Table 3: Summary of interview participants

they trust enough to share these devices with. id137 mentioned: *"I wouldn't share it because my family doesn't live close. Do not trust that many people. Neighbors are not close enough for me to allow them to access any of my home devices now or in the near future."*

4.4 Sharing Experiences Beyond the Home

We conducted a follow-up interview with 13 smart home users who currently share their devices with people outside of their home to get a more holistic understanding of the factors they consider when selecting their community, their detailed sharing behaviors, as well as their concerns and needs. In this section, we describe our participants, and an in-depth analysis of the themes that emerged from the interviews.—

4.4.1 Participant profiles

Our interviewees consisted of 9 male and 4 female participants who currently share one or more of their smart home devices with at least one person who does not live in their house. Nine of our participants live in a single-family home, four others live in an apartment. Eight of the participants are home-owners and the rest rent the place where they live. The descriptive statistics of our participants are summarised in Table 3, along with pseudonyms for each participant that we use throughout this section.

We first provide a detailed description of our participants and why and how they share their smart home devices. We group our participants based on their needs and uses for sharing their devices with people outside of their home. As participants' motives for sharing varied, the same participant can appear in multiple groups below.

Keep in touch

Five of our interview participants (Lucia, Travis, Ben, Mark, and Joe) share their smart speakers with close family members, i.e., parent, sibling, children, and close aunt, for communication purposes. Joe, a 48 years old healthcare professional lives with a roommate and shares his smart speaker with his son, as well as his roommate's in-laws. Lucia, Travis, Ben, and Joe each discussed the advantages of using the Drop-in feature available in their Amazon Echo. Travis lives with his parents and younger siblings and shares the drop-in feature with his aunt and sister because: *"It's helpful in a sense that if the kids just got home from school and my parents or I have to run and get something, they can just have someone like there speaking to them that's an*

adult figure."

Lucia shared her Amazon account with her mother even before she bought the Amazon Echo. Her mother now uses the speaker to help her take care of the kids and buy household necessities. Ben and Joe also share their accounts with others in order to share their calendars, plans, and music. Travis, however, is a bit uncomfortable with his aunt having full access to his account. He does not like his aunt having access to the audio logs because *"(she) keeps looking through what's been said... just comes to a point where it's just a little nosy."*

Safeguard the house

Eight of the interview participants (Abby, Jim, Eric, Matt, Daniel, Ben, Mark, Joe) share their smart doorbell, indoor camera, thermostat, burglar alarms, and fire & freeze alarms so that others can monitor their home, especially in their absence. Travel initially triggered the sharing of these devices for Abby, Jim, Matt, and Daniel. Daniel, a 26 year old IT engineer, shares his smart thermostat with his close friends and parents because: *"I usually go on vacation in the winter-time. So if it gets super cold, and I'm not home, say a big, you know, for whatever reason there's a cold snap or something like that, my friend can just keep an eye out on it and see, make sure that the temperature sensors in the different rooms aren't getting too cold and if they are, they can adjust the heat that way my pipes don't freeze."* Matt, a 29 years old analyst, shares the account information (username and password) of his indoor camera with his friends and siblings when he goes on a vacation, even though there is a shared user feature available in the app because he thinks it is easier. He disables access

by changing his account information when he comes back from vacation. Similarly, Daniel, shares remote control capability for his devices when he goes on vacation, and changes sharing back to view-only capability when he returns.

All of these participants except Ben share the devices with close family members and friends who live near to their home, because those people will be able to quickly respond to an emergency. Violet, a 39-year-old homemaker, mostly stays at home alone with her kids because her husband has long and late work hours. She shares her smart doorbell with her uncle: *"We live kind of far from where we grew up, me and my husband. I mean probably like 30 miles from where we grew up, so most of the people and most of our other family are still very far from us. My aunt and uncle live probably about two miles. So it's really just safety. It's so if there was ever any trouble my uncle could see it right then and there and come to my rescue."* Eric and Ben share their alarms with family members who do live far away, but who can still help notify appropriate people in case of a break-in or fire.

Mark wanted to share his smart doorbell with people other than his brother, while Amber wanted to share her fire/freeze alarm with someone to enhance the security of the house. However, both of them reported not being able to share those devices because manufacturers do not provide fine-grained sharing options that satisfied their needs.

Help with pets

Four participants (Lucia, Amber, Max, Ben) share their smart indoor camera and thermostat so that other people could monitor the safety of their pets. Lucia, a 38

year mother of three shares the smart thermostat with her parents and a sibling: *"I'm busy with the kids; she can check the temperature and make sure it's not too hot, or not too cold or turn the air on, or something. Because we have cats that are sometimes home alone. So, it's just helpful to have somebody else, have another set of eyes on the thermostat when we're not around."*

Amber enthusiastically shared her pet camera for the first time when she went on vacation for four days. She made her pet cameras public and posted them on Facebook so that her friends and family members could monitor the pets and play with them in her absence. She is not particularly concerned with making her indoor camera public to everyone because the cameras are not in a private place in the house. She makes the cameras private again when she comes home. Max and Ben also first shared the live streaming of their indoor camera with their family members before traveling to keep an eye on pets. However, neither of them revoked access when they came back because they only allow close trusted people to view live streaming.

Provide easy access

Six participants (Abby, Eric, Amber, Daniel, Ben, Joe) share their smart lock, smart lights and/or smart doorbell so that their friends and family members can easily access the house physically or virtually. Eric and Daniel want their friends and family members to remotely turn on lights, especially at night and if the house is empty. Abby, a 31 year old teacher, shares her doorbell with her mom because: *We go on cruises a lot and so we're out of the country and so she can set notifications on if somebody rings our doorbell... She can also answer if somebody rings the doorbell*

and talk to them.

Ben and Amber share the lock/unlock capability with their parents and close friends, so they can come to the house anytime or open the door for someone else when they are not home. Amber also shares a temporary key with the pet-sitter before she goes on vacation. She is quite happy with the fact that she can just activate and deactivate the same key anytime she wants instead of creating a new one each time she leaves. Daniel instead creates temporary keys for the people who come to visit and does not provide continuous and remote access to his smart lock to anyone.

Eric, a 37 year old IT professional, shares remote control of his lights and locks with a close friend who frequently visits and also has a physical key to the house. Eric explained that since his wife is not tech-savvy, his friend, who also works in IT, can serve as a backup person to troubleshoot the devices when he is not available.

4.4.2 Trust mediates sharing

For our interview participants, their trust relationship with the people they share devices with plays an important role in their sharing behaviors. Almost all of our interview participants mentioned they explicitly and completely trust the people with whom they share and firmly believe that they will not misuse the shared devices. For instance, Lucia said,*"She's (mother) one of those people that will always let me know what she's doing ahead of time. I mean she could accidentally turn the thermostat up or down. But I don't really think she would do that. She's a careful person."*

Daniel justified why he would trust his friends more than his neighbors with his smart home devices by saying: *" I've known (friends) for a minimum of 10, 12 years,*

you know, some closer to 20. So, yeah, more of a I guess a trust thing. You know, my friends will let me know, like if their phone gets stolen or something, you know, that way I can just disable their access. If my neighbor loses her phone, I don't think that they're gonna call me to tell me, Hey, I lost the phone."

Four of our participants (Abby, Jim, Max, Violet) explicitly mentioned that they would not share their smart home devices with anyone else in the future outside of their current trusted community. Thus, these results reflect similar comments provided by survey participants that they chose people to share with because they were trusted, and would not share with those who were not sufficiently trusted.

4.4.3 Sharing full access

A number of our participants (Lucia, Travis, Jim, Matt, Daniel, Max, Joe) shared their account information or full administrative access for at least one of their devices because it was more convenient and easy to do with their trusted community. Travis justified sharing the account information for his smart speaker by saying: *"If they wanted to they could change the password and stuff like that... It's only in case someone else gets locked out of using it so I can have someone else to try and get in, see if that would work. It's more like a fail-safe kinda thing."*

Matt shares the account information of his indoor camera, even though there is a shared user feature available in the app, because he thinks it is more convenient and he configured his account and device to alleviate any concerns: *"I have it automated at this point so that when I come home, the camera (Wyze) automatically shuts off. When I leave home, it automatically turns on based on some present sensors... also*

there's no personal information as well as financial or health any PII related information that is on the Wyze account itself. So worst-case scenario, all I have to do is reset and change accounts." Max, on the other hand, did not have an option of adding shared users to his camera, but he was *" fine with having just username and passwords for all cameras without the ability to restrict anything. I am comfortable sharing it in that manner (only live steaming view) with parents and siblings because I trust them."*

Daniel, despite having a more nuanced sharing preference than most of our participants, shares full admin access of his lights with his parents when he goes on vacation because: *"It's just quicker and easier to give them (parents) full(admin) access than to create a defined level of permissions for something so temporary."*

In other words, some of the participants want to share full access to their devices. And others just found it easier to do so, and were comfortable with providing complete access because of the trust they have in those people.

4.4.4 Fine-grained controls may mediate future sharing

Though our participants were not particularly concerned about their current sharing practices, five of them (Travis, Eric, Amber, Ben, Mark) did prefer to have more nuanced sharing controls on their smart devices.

Eric works as an IT professional and created a custom controller to share specific capabilities of his smart home with others. Ben, on the other hand, wants manufacturers of smart devices to provide options to create delegates such that: *" I can give access to any contact that I want and then I can control the degree of access that I*

want them to have. So if I want them to have access to maybe a camera for live viewing, but maybe I don't want to give them access to all the historical, especially from outside of the home...Let's say that someone's keeping an eye on an old person or somebody who's got some mobility issues, but you don't want them to see historically every single time they take a shower or anything like that."

Amber explained how not having enough control is affecting her current device sharing decision: *"It (Nest Home app) says, You can invite your family members to join your home. So I have Nest Fire, it's called Nest Protect. It's the fire, the smoke detector. The problem is that I just looked at my app, and it says, "They will have full control over your device." Well, I don't want that. They can remove them, they can add them. That's not what I want. I just want them to be notified in case the smoke alarm's going off."*

Moreover, Mark mentioned how more subtle sharing controls would support future sharing: *"I don't think I would let anybody else use it (doorbell). Because for the Ring, you have access to everything, but if there was a way I can send a one time link to a person so I could ask them to check over my house. If there's anything going on over there? If they made something like that, then I would probably let someone else have that access."*

Yet a challenge to providing fine-grained controls is users' understanding of what access they are granting. Many participants were uncertain over exactly what other people could access, which would be critical if granting access to less trusted individuals. For example, Jim was confused about whether his son has the capability to share the videos recorded in the smart doorbell: *"I just am not familiar enough with*

the system to know if he can share that video clip or not...There's no audit trail... if hypothetically I had a neighbor, whom I would have given access to, then I would want to know when my neighbor would be accessing it.

4.5 Discussion and Implications

We first revisit our research questions to summarize the results of our survey and interview.

RQ1: Are smart home users interested in remotely sharing their devices with people who do not live with them? The answer is a resounding yes! Sixty-four percent of our participants either already share or are interested in sharing their smart home devices with people who do not live with them. These people are close, trusted community members who often live near their home. Participants chose to share with people that thought to be trustworthy, knowledgeable, and capable of interacting with their devices. Participants also expressed a desire to share in this responsibility by having access to others' devices as well.

RQ2 and RQ3: What devices and for what purpose? The overarching goals of sharing were to receive assistance in the care of and access to the home and its occupants. The devices shared were the ones that were useful for these goals within different homes. Thus, cameras were shared to enable remote check-ins on a home and pets; alarms and security systems for monitoring of emergencies; locks and doorbells to allow access to the home; lights and locks for home security; and speakers for communication. While our results highlight commonly desired capabilities, various participants expressed a desire for all capabilities, depending on their needs. And

some shared with others who could help with device configuration and maintenance itself. Thus, we would expect that some people would want to share access to the entire range of smart home devices, even those we did not explore in our study, for similar purposes.

RQ4: What are the sharing experiences and needs for those who already share? In both our survey and interview results, participants indicated that they often shared full access to devices with a set of trusted people. They utilized the simplest method they could to enable access, including giving full account credentials to friends and family. Others simply enabled or disabled complete sharing as needed, such as turning on or off camera streaming while traveling. While this full access was not always necessary, participants were not concerned for the privacy of their information or homes because of the level of trust they had in those they shared with. Still, participants expressed unmet needs for more fine-grained control of sharing capabilities in order to share with other people who are less trusted. This is consistent with findings by Brush et. al that indicated that participants would be willing to share with neighbors if the boundaries of sharing are clear [23].

Thus, the overarching result of our study is that people are interested in allowing access to their smart devices to share the responsibility for the safety and care of their home and inhabitants with a close, trusted community of people. These needs trigger sharing, and the lack of need or of trusted, capable people inhibits sharing.

Unlike prior research which identified nuanced access control desires for different audiences [39, 90], our participants currently rely primarily upon the all-or-nothing access that is standard with most IoT devices. Participants were willing to, and often

already did, share full and complete access to their devices with their most trusted family and friends, yet sometimes did so in ways that were not necessarily designed for such sharing. Results also highlight the challenges that participants faced in figuring out exactly what other people can access when using existing sharing interfaces. Interview participants expressed uncertainty in exactly what others could do with their devices, and in examining survey results, we believe many respondents were similarly uncertain. This may be another reason that participants only conceived of sharing with those they trusted the most - because they were not sure of the access they were granting, they could assume that all access was possible and be comfortable with that possibility.

Despite the prevalence of sharing already, there were unmet needs for sharing with people outside of this close trusted circle, for the same purposes. These people included additional friends, neighbors, and other house help that could also participate in the monitoring and care of a home. Survey participants who were not interested in sharing often expressed reasons of not having any trusted people in their nearby communities. A number of interview participants mentioned scenarios where they would require finer-grained control in order to allow device sharing with additional people, but with only selected or temporary capabilities. One tech-savvy participant even built his own fine-grained access control system for his smart home. Thus, as others have also identified [48, 51, 90], users do need methods to allow for more restricted forms of sharing, to enable the expansion of users they could share with and the community which they can rely on to help them with their homes. The challenge will be to design mechanisms that are sufficiently easy, and allow users to have knowledge

of and confidence in the access they are providing. We believe that designers could be informed by the common goals and responsibilities of various circles of community members that smart home owners rely upon.

4.6 Limitations

Similar to other survey and interview studies, our study is limited in generalizability due to convenience sampling from the Qualtrics panel and smart home-related IoT forums and limited sample size. Participants were also drawn solely from the US. However, we tried to maintain the ecological validity of our study by recruiting only existing smart home users and asked questions based only on the devices that they currently use.

Sharing behaviors in both the survey and interview are self-reported, and are not necessarily accurate. We did not more deeply investigate the views, concerns, and needs of people who have thus far refrained from sharing, even though in some cases they desire to do so. Future studies should examine concerns and need of smart home users who are reluctant to share their smart home devices with people outside of their house.

4.7 Conclusion

In conclusion, our study demonstrates that many users are already sharing their smart home devices to enable close, trusted friends and family to help monitor and remotely control their homes. While people are generally comfortable providing full and complete access to this trusted community, they do not necessarily need or desire to do so. More nuanced and restricted controls may enable additional sharing with a

larger community, yet creating such easy-to-use controls remains challenging. These results provide implications for designing new control mechanisms to improve the capabilities of smart home sharing beyond the home.

CHAPTER 5: EXPLORING END USERS' SECURITY AND PRIVACY CONCERNS, BEHAVIOR AND NEEDS IN CONTEXT

In the previous sections, I have reported the results of a survey and multiple interview studies on end-users' perceptions, concerns, and needs around managing their data and social privacy in the smart home. These studies helped me to identify end-users' perceptions of security and privacy risks from sharing their data and devices with multiple stakeholders. However, because of the retrospective nature of these studies, it did not provide much insight into how people make security and privacy decisions at the moment when such incidents occur and what factors they consider when making those decisions. Hence, as the next step to my investigation, I have conducted a combination of experience sampling study and interview study to understand what privacy means for smart home users when they are actively using the devices in their home, what their considerations are, and how they act on those considerations. Our research questions include:

- RQ1: What are end users' in-situ privacy considerations, behaviors and needs?
- RQ2: What factors elicit those privacy considerations?
- RQ3: What privacy mechanisms are needed to support users' in-situ privacy needs?

5.1 Methodology

In our study, we have utilized two complementary methods. First, we have conducted an experience sampling study (ESM) that lasted for two weeks. ESM is a research method to collect data from participants about their experiences in daily life as they occur. We have used this research method to gather more ecologically valid and accurate data as participants would be logging the events as they occur. After that, we conducted a follow-up semi-structured interview study with the participants to get a more detailed understanding of the ESM study logs. The study was approved by our university Institutional Review Board (IRB).

5.1.1 Recruitment and participants:

Participants were recruited from advertising our study in smart home-related groups on Facebook and Reddit, as well as the university's mailing lists for faculty and staff. Participants were asked to fill out a pre-screening survey answering what type of smart devices they have in their house and how often they use the devices. We conducted the experience sampling study via a smartphone application called PACO [4], which can only be accessed through a Gmail ID. Hence, we have also asked participants in the screening survey whether they are comfortable using the app with their Gmail ID for the period of the study. Finally, participants were asked whether they would be willing to participate in a follow-up interview.

We recruited 30 participants who own at least three types of smart home devices, use smart home devices every day, and were willing to use the PACO app and participate in a follow-up interview. All of our participants live in the United States

ID	Gender	Age	Profession	Number of (concerned) logs
P1	M	32	Administrator	7
P2	M	26	Research Scientist	5
P3	F	23	Sale associate	17
P4	F	36	Student Affairs	3
P5	F	23	Student	2
P6	M	29	Registered Nurse	5
P7	M	35	Driver	3
P8	M	41	Project Manager	6
P9	F	21	Student	3
P10	F	34	Student	4
P11	M	36	Shipping Clerk	4
P12	M	36	Senior Media Specialist	4
P13	M	55	Client Solution	1
P14	M	37	Project Manager	4
P15	F	54	Editor	4
P16	F	26	Student	1
P17	M	67	Retired Engineer	1
P18	F	57	Retired	2
P19	M	36	Service Provider	3
P20	M	57	Media Producer	1
P21	F	40	Human Resource	3
P22	M	71	Retired	11
P23	M	24	Information Security Specialist	10
P24	M	46	Teacher	3
P25	M	54	Engineer	3
P26	M	21	Student	5
P27	M	30	Student	3
P28	M	23	Student	2
P29	M	22	Student	8
P30	No interview			5

Table 4: Summary of the participants

except P23, who lives in Canada. Table 4 summarizes our participants. All the participants completed the experience sampling study, and 29 of them participated in the follow-up interview. Participants received $20 for completing both of the study components.

5.1.2 Procedure:

We collected two weeks of experience sampling data via the PACO app. PACO is an open-source platform for behavioral research. We have decided to run our

study through the PACO app since it travels with the participants all day on their smartphones and provides flexible options to prompt users to log data necessary for ESM studies. The app reminded the participants to log their experience with the smart home devices once a day, at a randomly chosen time. The log was collected as a form of answers to the following questions:

- How long ago was your most recent interaction with one of the smart home devices?
- Which smart home device did you interact with most recently?
- How did you interact with the device?
- What was the purpose of that interaction?
- During that interaction, did you think about or have any concerns with any of the following? (select all that apply) [The information that is collected, How your information is stored, How your information or device will be accessed and used by others, What can be inferred about you by others, None of the above]
- Did you have any privacy considerations or concerns during that interaction? [Yes, No]
- If Yes, What did you feel, and what made you feel that way?

Participants were also asked to log any interaction with their smart home devices that made them think about their privacy, and they were encouraged to do so as soon as such interaction occurred. In other words, participants could log their experience whenever they wanted without any reminder.

At the end of two weeks of the experience sampling period, we conducted a telephone interview with the participants to get an in-depth understanding and ask follow-up questions about the logs. The participants were prompted to describe the incidents they logged in detail, especially what triggered them to log, how did they deal with the incidents, and finally, what support they needed at that moment. We recognize that our study may make participants more conscious about their privacy with smart home devices. Hence, we explicitly asked participants to discuss any concerns or considerations triggered by the study. Finally, we asked demographic questions at the end of the interview. The interview was audio-recorded and lasted for 32 minutes on average.

5.1.3 Data analysis:

We have run descriptive analysis on the close-ended questions of the reported logs. We used the logs as discussion points in the follow-up interview to understand the circumstances around the privacy consideration, end-users' behavior towards those considerations, and their needs. We have transcribed the audio recording of the interview. I did inductive coding on several interviews and built the initial codebook. The codebook was then discussed and finalized by all the researchers. The final codebook consisted of 12 structural codes. The researcher used this codebook to code the rest of the phone interviews.

5.2 Results

In this section, we present our findings. We begin by providing an overview of the instances reported in the ESM study, particularly the type of device that elicits

considerations. After that, we will provide an in-depth analysis of end users' considerations, beliefs, and behaviors that emerged from the ESM study and interview.

5.2.1 Overview of the reported logs

From the 30 participants, we received 504 logs in the two weeks of the experience sampling study. In 133 of them, participants reported some considerations about their privacy in the smart home. From now on, we will only report on these 133 logs. The number of such logs per participant ranged from 1 to 17 and is reported in table 1.

Participants reported several considerations related to different smart home devices. The most frequent one is the smart speaker (67 logs). Participants mostly talked about the always-listening capability of these devices and how that leads to some feeling of intrusiveness. P12 shared his experience: *"Both my wife and I have noticed that where we've had conversations about things that we want or something like that, but we have not searched on Google or anything like that. And then we notice on Amazon, or like in our email, will get like "You might be interested in this product" after we've had a conversation about it or we've seen targeted ads on Facebook..., and that's always really, really weird. It made my wife ask the question actually like, "Is the echo always listening?' "*

The other logged devices are those that provide physical security of the home (24 logs), such as a smart lock, alarm system, or motion detector. Participants were mostly worried that these devices could be hacked to get access to the home. Participants also reported on devices with a camera (21 logs), such as indoor/outdoor

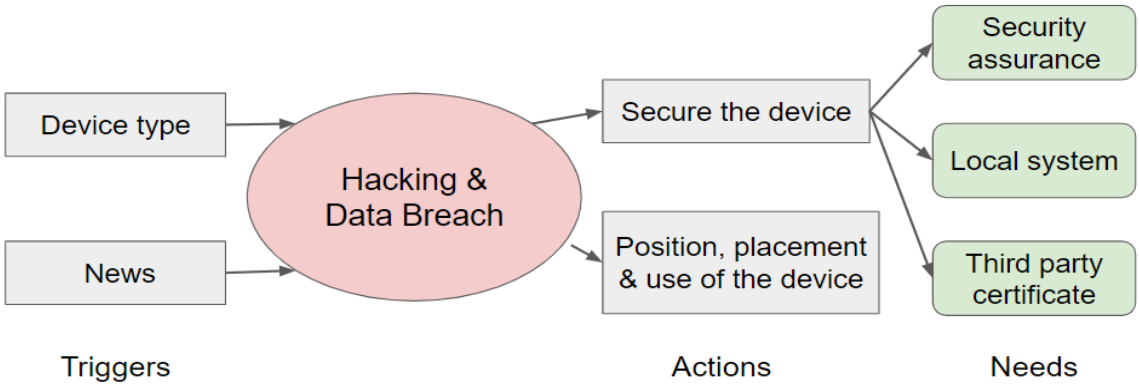


Figure 6: Hacking and data breach: triggers, actions and needs

security cameras and doorbells, with similar hacking and security breach concerns. Furthermore, there were logs about interactions with different appliances (18 logs) such as lights and vacuum cleaners. Participants thought about how much of their life could be inferred from these devices. For instance, from the pattern of when a light is on or off, it can be inferred when someone is home or not.

5.3 Privacy considerations

The analysis of both the ESM and the interview data revealed a number of data privacy considerations caused by several factors and experiences of the end-users. Participants managed these considerations by taking several actions. In this section, we will report on end-user experiences, activities, and needs surrounding these considerations. Afterwards, we will present several additional themes that emerged from the study

5.3.1 Hacking and data breaches

Not surprisingly, most of our participants shared their concerns about the possibility of the devices being hacked and controlled by a malicious party. Participants also

discussed the potential of a security/data breach that would lead to unauthorized access to private data. These considerations were mostly triggered by participants owning particular devices, especially smart door locks and smart doorbell/cameras. Participants also think about these security threats when they hear about them from external sources such as news, forums, and social media. For instance, P5 mentioned: *"When all of the hacking issues were going on recently with like the gas pipeline, big companies... it just made me think how someone could easily hack into the website and see like the pass-codes for all of the doors, for all the houses that are run by that company."*

Participants did not actively take any actions when such thoughts came to their minds. Instead, all of them made some decisions about the placement and use of the device (i.e., not placing the device in a personal space such as a bedroom, using the camera only when not home) when they first started using the device. For instance, P29 discussed that: *"The vacuum robot has an image sensor that maps your whole house. So it can see what I was doing this morning while it was cleaning. It's like a security camera in your house."* and he uses the robot only when no one is in a room. Furthermore, participants also discussed several standard security measures they employed, i.e., separate and secure WiFi for smart devices, two-factor authentication, strong passwords, updating the software, covering the camera lens, building/using a local system, etc.

Our participants were comfortable with how they are currently using their devices. However, the concern about security breaches and hacking is always in the back of their minds. Our participants believe it is the responsibility of the device manufac-

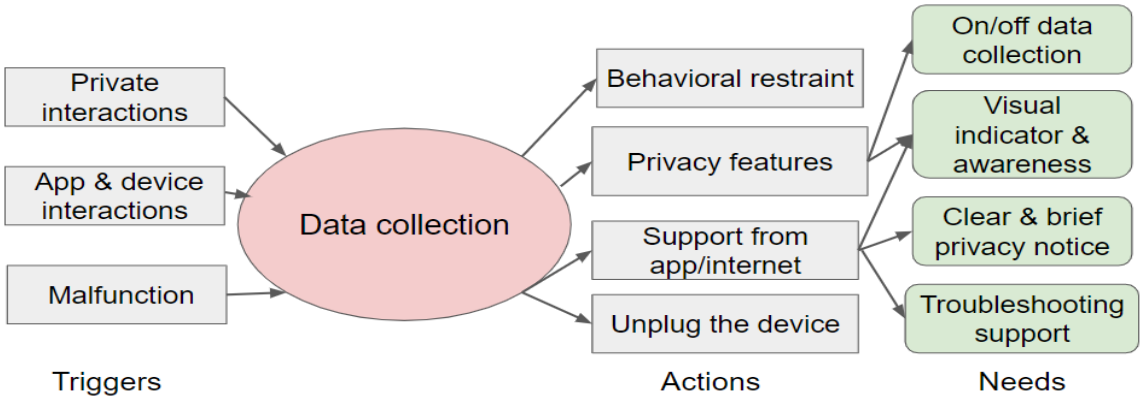


Figure 7: Data collection: triggers, actions and needs

turers to provide proper security to the device and the back-end cloud server. Several technical participants suggested other measures that would provide more peace of mind to smart home users. The first one is providing support to build a local smart home system, i.e., the ability to store recordings in a local SD card, open-source the product, etc. For example, P1 mentioned:

"it allows an end-user to look at things and say: Okay, this has all of the specifications that I need. It's going to work with everything I need. And so, I can use that information to build my own system and trust it is secure, feel that it's secure, and know that people are making their own patches and modifications."

The second measure they discussed is a third-party security certificate for the smart home devices, *"all these devices had to adhere to specific security to earn this seal of approval from some company that was nonprofit, and that was recognizable enough that that would be something that you actually look for (when buying the device)(P20)."*

5.3.2 Data collection

As discussed before, participants considered that some devices would collect potentially sensitive data, such as smart speakers and cameras. They accepted the data collection when they decided to use these devices and developed practices to become comfortable with that. However, our participants shared several events that led them to think about the data collected by these devices:

Private interactions: Participants thought about data collection when they have any interaction in front of or with the device they consider private. Examples of such interactions are having a private conversation or doing personal activities in front of the device and using features such as Drop-in and phone calls. Participants normally act on their concerns by showing behavioral restraint (not having a personal conversation, limiting the use of the features) For instance, P21 mentioned:

"I go on walks with my neighbor, and a lot of times, like before we start walking, we're standing outside my house, having a conversation. You know how sometimes you've been talking like that about your partner, and then I'm like, oh, I hope he doesn't see this. So, I try to meet her like farther down on the driveway, let's move out of the range, you know."

A few of the participants also mentioned using available privacy controls. For instance, P4 mentioned: *"I have one Echo that's in a bathroom for playing music like we're in the shower. It's always on mute (using the mute button) until we're actually actively going to use it. I just don't want to record me going pee."* These participants wanted an easy way to turn off/on data collection both from the device

and the associated application when such events occur. For instance, P10 expressed her struggle with the physical mute button: *"I have a little difficulty for Mobility. It's not very convenient for me to physically turn off the button. If the button is in the app, it would be more convenient."*

Malfunction: A number of participants experienced device malfunction where the device was behaving in an unexpected way. For instance, the ring got stuck in the smart speakers for both P3 and P11. P3 accessed the app, hoping to find some information about the malfunction and how to troubleshoot. However, she did not find any info and unplugged the device as she was concerned that it was recording. P11, on the other hand, found that his MacBook was connected to the echo via Bluetooth. He said: *"my concern was that the device was trying to do something...it was trying to connect to something I didn't ask it to connect (or do not remember asking) and anytime that kind of happens, You're wondering, you know, what else is happening? And I do not even hear a tone. there's a lot of different things to be done with Bluetooth, like transferring files."*

He also discussed the difficulty of troubleshooting in the app when such a malfunction occurs: *"When I was trying to figure out okay, why is this connected to Bluetooth? You know, I'm probably tapping the app on my phone seven or eight times just to get to that kind of where that information is and guessing, too, right? So I'm like, well, is it under this subcategory? How do I figure this out? The interface to the app is confusing, and sort of it consolidates all your Echo devices into one app and doing so, you've got a lot of different features turned on and off within a lot of different sort of tabs through the app. So until I figured it out, I unplugged it."*

Participants discussed the need for a user manual both in the app where *"they include a little section for troubleshooting that says, specifically like where you can find in the settings if you have like a problem and how to fix that(P3)"*.

Interaction with device & app: Participants were prompted to think about data collection through their interaction with the device and app. For instance, P3 and P18 noticed that Echo knows their location when it reports weather; P10, P18, and P4 found out echo stores the audio interactions; P24 realized that the outdoor camera picks up audio from inside the house and records neighbors; P15 recognized the extent of data collection from looking at recordings shared in the neighborhood app. P15 mentioned:

"Usually, just from the information that people volunteer (in Ring neighborhood), I have a pretty good idea of what's happening where. But it's the identity of a particular person. Somebody could send a picture of me, delivering packages and it would go up to like a mile radius of my home as me holding the package."

Some of them acted on these events by looking at the app or internet for more information and taking some actions to reduce data collection. For instance, P3 looked at the Alexa app to make sure it was not using her phone's location, P10 investigated whether echo records her phone calls, and P4 deleted all the recordings. P24 found and used the option to turn off audio and turn on a light in the camera to make people aware that the device was recording. He also planned to use the Home Away feature (record only when not at home) to "limit some of the recordings that (are) being done" but didn't do it because it was not free.

P18, on the other hand, was frustrated for not knowing that Echo was storing the

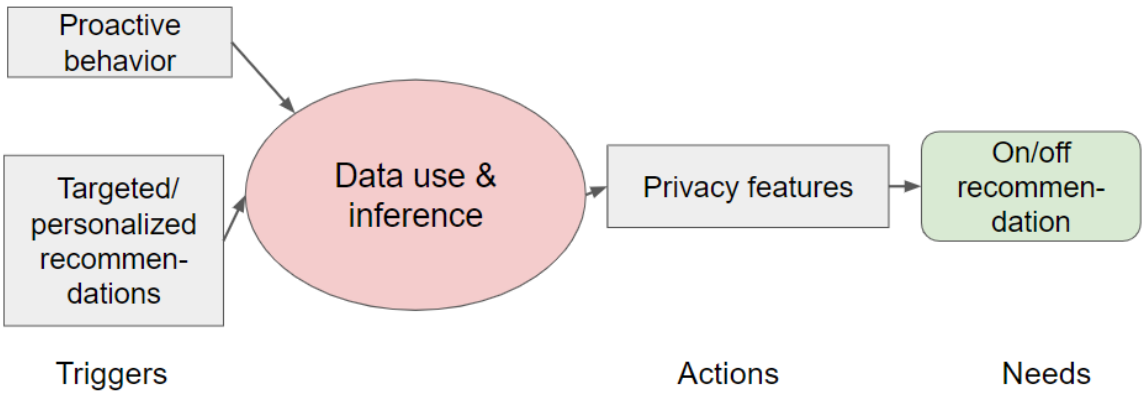


Figure 8: Data use and inference: triggers, actions and needs

audio interaction. She said: *"They should put that information somewhere. It should be part of that quick set-up guide when they give you instructions because you do read it to learn how to hook it up. Periodically, when you open up that Alexa app is a bunch of tips, like things that you can do. They should have it in there as well like all interactions with Alexa are being recorded and stored; you can access it here."*

To summarize, participants discussed the need for the app to provide: 1. precise information on what major data points (i.e., location, audio, video, etc.) are being collected and stored; 2. Options to easily turn on/off such data ; 3. Awareness of what controls on data are available and where to find those controls in the app and in the device's box; and 4. Having these controls free of charge

5.3.3 Data use and inference

Our participants believed that the manufacturers use the data collected by the smart home devices to make inferences about the user and build their profile. Several incidents elicited the thought of data access, use, and inference, as discussed below.

Proactive behavior: Several of our smart speaker owner participants reported

their experience with the devices to act proactively without them initiating interactions. For instance, P6 received a recommendation from his thermostat to switch to eco mode to conserve energy. It led him to think about whether the energy company has access to the data. P21 shared his experience of a proactive suggestion from her echo: *"it was about a book. It was like an author you follow has a new book. Do you want to add it to your wishlist or whatever? And I am thinking about going in there and changing it. I want to initiate, you know, what information I'm looking for from her instead of her just trying to get me to purchase things off Amazon."* P21 expected to find an option to turn off recommendations in the app, whereas P12 believed that: *"there is not very much we can do about the recommendations and stuff. I don't think there is an option to turn it on or off, you know, it's just part of having it in our house."*

Participants viewed proactive interaction as an annoyance rather than being overly concerned about how their data was being used. Yet, all of them wanted to have an option to turn off proactive suggestions from the application and plan to use that, especially participants who have received purchasing recommendations.

Targeted/personalized recommendations Receiving personalized service from the device and targeted ads on the internet made several of our participants consider how their data are being shared and used. For instance, P12 mentioned: *"I have noticed targeted ads on Facebook and other social media that seem to correlate not with google searches but with things we mention to our echo. "*

P25 received a personalized energy efficiency report from his thermostat, which led him to think about who else has access to that data and what conclusion could be

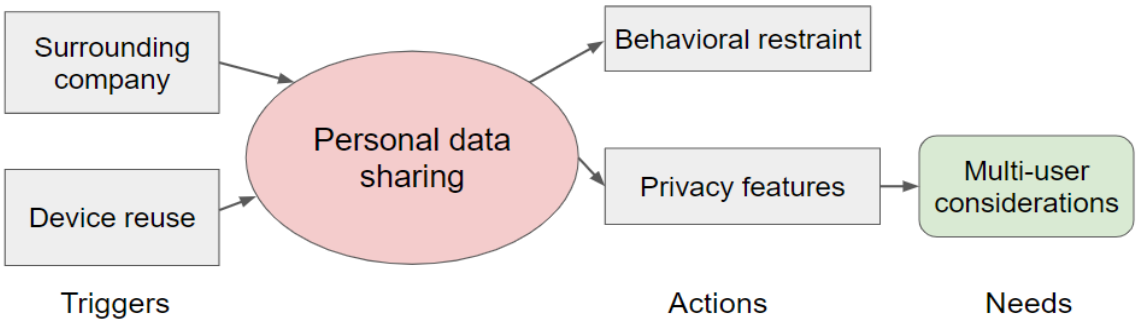


Figure 9: Personal data sharing: triggers, actions and needs

made from it about his life. Our participants believed there was not much that could be done about this issue other than accepting it because *"if you're limiting that risk and exposure, then you're also limiting the benefit. (P18)"*

In addition to the instances mentioned above, several of our participants discussed that they think about the data collection, use, and inference when they decide to buy or start using a new smart home device. Several also mentioned taking some actions at that time. For instance, P2 decided to buy smart home devices only from google, so his data is within one company. P14 used the option in the app to not *"allow them (Amazon) to review the recording or share recordings."* However, they said these thoughts become very infrequent as they get accustomed to using the device.

5.3.4 Personal data sharing:

Some of our participants shared their experiences where they were prompted to think about or experienced other people having access to their data.

Surrounding company: Participants reported different methods to reduce personal data sharing when multiple people may have access to the device. For instance,

P2 mentioned using voice recognition so no one else can access her calendar, emails, etc. P27 decided to use the smart weight machine when no one is around because it gets connected to the nearest phone through Bluetooth and reports the weight. Yet, some participants discussed unexpected sharing of the data when other people were present while using the device. For instance, P3 had company when she got a notification alert from the Echo. So, she asked Echo to turn off the notification, and Echo read out the notification before turning it off. She tried to fix it from the app but could not figure out how to do it. The device behaved unexpectedly for P3, whereas for P27, his roommate overheard his interaction. He shared his experience as:

"the door was open, I set the alarm and then my friend told, Oh, you're awake too early, are you going to go somewhere tomorrow or something like this?" He wanted the device to understand the lower tone and set up a repetitive alarm to reduce the chance of others hearing his voice interaction.

Device reuse: A few of our participants were renting a house or apartment that came with some smart home devices. These participants considered what would happen to their data once they moved out. They wanted the device to be reset and all their data deleted at that time. However, P5 mentioned: *" I think the company that owns the house, I think they would do it. I don't think I have access to it (delete the logs), reset it, or anything."*

5.4 Emerging Themes

5.4.1 Distrust over company

A common theme that emerged from several participants is their distrust of the company. These participants believe that the companies will find a way to accumulate and use user data, and there is no way to limit that. For instance, P7 mentioned:

"There is always that very long thing that you have to agree to, that nobody ever reads. Even if they put something in there because there are so many loopholes and they have their team of lawyers, and you know, they're going to get what they want. So, I don't think anything can be done to make you trust that no one's keeping your data."

Some of these participants also believe that even though they delete the data from the app, it will still be stored in the cloud. Therefore, they do not see a reason to delete the data from the app. Even when the company explicitly says that they remove data from their server once the users delete it, participants were concerned that companies might violate what they are saying. For instance, T8 mentioned:

"Even if they did come out and say that: 'we are not recording, we're not saving, we're not listening.' I probably wouldn't believe them. So, given that I don't think there is a resolution to that concerns there."

P7 & P28 shared similar distrust over the mute button in Amazon Echo. For instance, P7 mentioned:

"On the devices, you can push the with a mute button or turn off the microphone button. But again, at that point, you're still trusting the device to do what it's telling

you it's going to do, you know. you're trusting Amazon to not just put up a red LED versus.. you're trusting that they're actually turning off the device"

Similar considerations emerged when participants talked about the possible use of their data for advertising purposes. For instance, P17 mentioned: *"they're doing the same thing gathering data. It is for advertising, and I'm sure that's where they're making their money. You don't sell the device for $20, let it run for years on your cloud or somewhere else without making money."*

5.4.2 Lack of awareness of privacy settings:

A number of our smart speaker participants were unaware that their interactions with the device are stored in the server, and they can review and remove those recordings. Some smart speakers came ready out of the box with very little setup necessary to use the device. The lack of interaction with the app, in general, hinders participants' awareness of data collection and available privacy settings. For instance, P12 mentioned: *"the common theme in most technology that we get in our house these days seems to be really simple instruction manual with almost no information. And I think that's to make people feel like they're easy to use. But I feel like you miss out on certain things like learning that you can go listen to your recordings and things like that. "*

Moreover, some of our participants looked at the available controls when they bought the devices and formed their understanding; however, were not aware of new controls released by the devices. For instance, P1 looked at the available privacy controls and tried to delete his recordings from Alexa when he started using it a

couple of years ago. He did not do it because the only option available was to review and delete the recordings one by one. He was not aware that echo now offers the option to delete all the recordings together.

5.4.3 Lack of access control in the central controller

The majority of our participants integrated their devices into a central controller (i.e., SmartThings, Amazon Echo) to control their devices. Some of them discussed the problem they face for the lack of granular access control in the central controller. For instance, P13 controls his devices with Smart Things and mentioned: *" I would like for you to use your smartphone to control the lights in our guest room, but don't control my life. Don't control my lights in my master bedroom. There is no greater personal granularity in the platform today. No permissions based or roles-based access into the environment".* He also shared his considerations with using third-party providers for access control purposes. He said:

"I got to use something like action tiles or another kind of third-party software and a tablet and create a custom dashboard that you can use, but that's a lot of work. (Also think about) integration with third-party providers and sharing my location for being granular."

5.4.4 Overwhelmed secondary users

Some of the participants discussed the issues the secondary users face who use the devices but have not bought or are primarily responsible for maintaining the devices. These participants are either secondary users themselves or the primary user (spouses or children of secondary users). The primary users in these cases are highly technical,

i.e., wrote custom scripts to automate the devices or build local systems.

P15, who lives with his spouse and two teenage children, was frustrated with the number of smart devices around her and the integration of these devices for doing everything in her household. For instance, she said: *"I don't really like using it for the TV or for the light, but sometimes I don't have any other choice, which I find frustrating. It (echo) doesn't always pick up my voice. So instead of just walking over and clicking the switch, I have to stand there and repeat the command several times just to kind of light on."* However, his family members like the way the device are automated. So, P15 had to adapt to her family members' choices.

P22, a primary user, had actively taken steps to improve the experience of his spouse. He mentioned:

"I've tried discussing how to make things easier for her, and for instance, on the patterns that Alexa recognizes, sometimes, she'll call a room by a different name. Just frustrated when it doesn't turn on the lights or something. So I got a label maker and labeled each one of them right there on the switch so she could see the names. I try to discuss with her before I put anything in or make any changes".

His wife, however, still worries about how to maintain these highly customized and automated smart home without P22. He mentioned:*" my wife's big concern is if I drop dead. She says I can't maintain this. I'm just going to sell the house."* P22 discussed the need for a third party who will listen to users' needs, evaluate them, and then would be responsible for installing and maintaining the smart home.

5.5 Design implications

In this section, we situate our findings within the existing literature and provide recommendations for improving end users experience in the smart home.

5.5.1 Support for privacy

Data privacy controls: Our study highlighted the need for easy ways to turn on/off data collection by smart home devices. Users need to use such features in multiple situations, such as to feel comfortable during private interactions, to limit bystanders' data collections, etc. Our results also show that this feature needs to be available both in the device and the app to make it more accessible to the user, especially users with special needs. For instance, P10 has mobility issues, and it is hard for her to mute her Echo using the physical button on the device. However, that is the only way available to turn the microphone off in the device.

Our study also shows users' considerations about the usage of their interaction with the smart speaker to receive unsolicited recommendations and targeted ads. Although users became accustomed to receiving targeted ads on the internet, they found receiving unsolicited recommendations from the smart speakers rather annoying, interrupting, and invasive. Proactive suggestions can be helpful in certain situations. For example, Alexa hunches alert users when the device is not in its usual state. If someone says 'good night, Alexa', and the lights are still on, Echo offers to turn them off. Alexa hunch is turned on by default, and users who find it invasive can turn it off. However, the suggestions from the smart speakers that our participants discussed were completely uncalled for, such as receiving information about the release of a new

product because the user bought a similar product. There is no option to turn on/off such unwanted interruptions to make these worse.

The smart speaker's users expect that the device will respond after the user initiates conversation. Such proactive recommendations mismatch users' expectations of how the device works. Hence, we believe it should be activated only when users explicitly opt-in for such a feature with a flexible opt-out mechanism.

Access control: Previous research shows that users want a more granular access control mechanism in their smart home devices. Our study adds to that finding by highlighting the importance of granular access control in central controller devices. We have found that several of our participants control the devices using the central controller app, hence interacting with that app instead of the app that comes with the device. However, the simplest access control features are often missing in such apps. For instance, in the Smart Thing, it is not possible to even provide device-specific access. The only way is to provide access to all or nothing. It is frustrating for the users, especially with kids, which is a very common scenario where someone may want to provide access to only some of the devices. There is sometimes third-party software available, such as Action tiles, to manage access controls. However, some users may avoid that because of their concerns with third-party software.

Furthermore, our study also highlighted the complexity of controlling access when the interaction modality is voice. Users may have other people in their surroundings, and voice interactions can reveal information that they do not intend to share. Manufacturers should design for privacy keeping such scenarios in mind, and design mechanisms to limit unexpected data sharing. For example, there is no way to turn

off notifications for one time in the Amazon Echo. The notification can only be turned off entirely from the Alexa app. However, users may have company and want to turn off notification only for that time or ask Echo to remind later.

Awareness mechanisms: Our findings confirm the previous research that end users are often not aware of the privacy controls available on the device. Ready to use devices with minimal setup, users' lack of interaction with the applications, complex app designs are some of the reasons for the lack of awareness. Our study also suggests that it is important to make new users aware of how devices work, what data they collect to and why they collect that data. For instance, P10 was confused about how her motion detector worked and ended up stipulating that it may have a camera through which it is actually detecting her movements. One solution could be to educate users about how the device works and what privacy settings are available when they buy and install those devices. For instance, manufacturers could provide a manual with the information within the box or make such information available at a part of the device set up. However, such awareness may not work when a third party installs the device and the owner is not directly involved in the setup process.

Furthermore, we have found that users seldom go back to the privacy settings of smart devices after their initial interaction with such settings, especially when they do not meet users' expectations. As a result, when these devices add new privacy features, users are often unaware of those settings. Traditionally, such awareness is provided via email or notification from the app. However, many users, especially the secondary users, may not have access to the email used to set up the device and only have the central controller app installed in their device rather than the device-specific

app. In addition to providing users with new data privacy controls, manufacturers should also think about how to make people aware as they release those controls.

Another issue identified by our study is the need for awareness of unused features or integrations resulting in unnecessary data collection. For instance, users may forget about the integration (Mac-Book is connected to the speaker via Bluetooth) and become uncomfortable when they get the awareness of that (unexpected notification from Mac-Book in the smart speaker). One option is to notify users if something is not used for a long time via the central controller app. Echo already provides hunches that alert users of the unusual device state. Such alerts could be helpful in this situation as well. For instance, smart speakers can notify a user that his Mac-Book is still connected to the smart speaker. However, users may perceive such notifications as unnecessary if they expect to have the integration. Hence, it is challenging to identify when to send such alerts to the users to be beneficial.

5.5.2 Support for Security

The majority of the users put the responsibility of security of their devices to the manufacturers. They have adequate reasons as it is in manufacturers' hands to keep the device secure by providing updates and patches, securing the data stored in the cloud, and putting security and privacy in the front of their development process. Manufacturers can support users by following security and privacy best practices.

Furthermore, some of our participants, especially with technical skills, had taken some of these responsibilities into their hands by creating their local system. They emphasized the difficulty of building and maintaining such systems. We argue that

manufacturers should provide flexible options for local processing and storage, considering all types of users. For instance, a non-technical user may consider having their camera recordings in local storage if such options are available, but be more comfortable with the device manufacturer managing the automation. In contrast, a technical user may want all the storage and automation processed locally. Hence, the device should offer different customization options for different types of users. Moreover, recognizing that most of the users are not knowledgeable about how to protect their own networks and storage, support should also be provided on how to customize the devices securely. For instance, if users decide to store their videos locally, educate and nudge them to use encryption.

Along the same lines, we have noticed that several of our participants relied on a third party to install and set up their devices. In many cases, all the participants do is install a central controller application in their mobile phone and use a given account credential to log in. Future research should look at who takes the responsibility of securing and maintaining the smart home devices in such a household and how the role of the third-party installers is integrated within that process.

5.5.3 Support for Malfunction

One theme that is emerged in our study is the lack of support from the manufacturers for suspected malfunctions. Users normally follow the easiest way to fix a problem, which is powering off the device and restarting. However, if that does not work in many cases, users do not know what to do. There is a lack of information available on why a malfunction happened and how to troubleshoot in that situation.

Although some companies such as Amazon provide troubleshooting information for specific cases on their website, such information is not available in the app, which is the primary means of interaction. Future research should focus on users' experiences, behaviors, and needs during a malfunction or unexpected behavior.

5.6 Conclusion

We have presented an experience sampling study with 30 smart home users examining their security and privacy experience. We found that although smart home users accepted the trade-off between security and privacy risk and convenience, they do experience situations that elicit their concerns. We have identified several factors that trigger users to think about their data in the smart home and areas of improvement in the current system to provide users support in such scenarios.

CHAPTER 6: INVESTIGATING END USERS' VIEWS OF SECURITY AND PRIVACY MECHANISMS IN THE SMART HOME

6.1 Motivation

Manufacturers have provided various awareness and control mechanisms for smart home device users to regulate these devices according to their preferences. The findings from chapters 3 and 4 highlighted that smart home users are often unaware and confused about the mechanisms designed to provide users more awareness and control of their data. It is unclear how smart home users utilize these controls, what considerations they make, and the implications of those decisions for users' privacy. 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 awareness of the privacy implications.

Therefore, we aim 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 a semi-structured interview study 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 [88, 80].

In our study, we have interviewed 21 non-owners and 18 owners of these devices to understand:

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

Our results reveal that users are mostly driven by the functionality when they configure their smart home devices. However, 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.

6.2 Methodology

To explore end users' perspectives of available controls in smart doorbells and locks, we conducted two sets of semi-structured interviews with owners of these devices, as well as users interacting with these devices for the first time. 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, which

we observed. We also interviewed participants who do own these devices, and asked similar questions about how they currently use the device controls. Both interviews centered on end user controls that are most related to privacy: those that configure awareness mechanisms and control what data is collected and how it is used and shared. In these two devices, these are controls related to notifications (i.e. turn on/off receiving notifications), data (i.e. view activity log and download, share and delete specific data points), and access (i.e. share the device with multiple people). The study was approved by our university Institutional Review Board (IRB).

6.2.1 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 these by distributing flyers in the nearby neighborhoods, and advertising the study in 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. For existing owners, we again advertised by distributing flyers in nearby neighborhoods, as well as posted in smart home related social media groups. These interviews were conducted over the phone, and audio recorded. All potential participants were asked to first fill out a pre-screening survey regarding the types of smart home devices they have in their house.

For the novice users, we recruited 21 participants (N1-N21) who owned neither a smart doorbell or smart lock, but may own other smart home devices. We refer to these participants as either non-owners, or novices, for the remainder of the paper.

ID	Gender	Age	Profession
N1	M	31	Title investigator
N2	F	59	Administrative associate
N3	F	53	Program coordinator
N4	M	46	CS Educator
N5	F	40	Educator
N6	M	33	IT professional
N7	F	57	Retail management
N8	F	31	Police officer
N9	F	51	Educator
N10	F	29	Education administrator
N11	F	29	Administrative assistant
N12	M	43	IT auditor
N13	F	51	Accountant
N14	M	40	Librarian
N15	F	33	IT professional
N16	M	63	Administrator
N17	M	34	Educator
N18	F	39	Administrator
N19	M	58	Engineer
N20	M	22	Campus minister
N21	F	63	Educator

Table 5: Summary of the non-owner participants

For the owners' interview, 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. 20 of the participants were male, and 12 of the participants were computing professionals. Note that we did not specifically target our own department in our university, yet we believe the topic of the study likely attracted a high number of computing professionals.

6.2.2 Procedure

We invited the participants who did not own a smart doorbell and lock 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.

ID	Gender	Age	Profession	Doorbell and/or lock owned
D1	M	56	Tram Driver	Ring doorbell
D2	F	30	Electrical engineer	Nest doorbell
D3	M	30	Service admin	Ring doorbell
D4	F	29	IT professional	Ring doorbell
D5	M	32	Investment banker	Ring doorbell
D6	F	53	Project manager	Ring doorbell
D7	M	32	Hospital admin	Ring doorbell
D8	M	47	IT security analyst	Ring doorbell
L1	M	19	IT student	Schlage sense & August lock
L2	M	35	Hospital admin	August lock
L3	M	45	IT professional	August lock
L4	F	47	Commencement coordinator	Kwikset lock
L5	F	30	Librarian	Kwikset lock
L6	M	37	IT professional	Schlage connect Z-wave plus lock
DL1	M	43	Cyber-security professional	Ring doorbell & Kwikset lock
DL2	F	54	Freelancer writer	Ring doorbell & August lock
DL3	M	50	Software Engineer	Ring doorbell & August lock
DL4	M	42	Web developer	Ring doorbell & August lock

Table 6: Summary of the owner participants

As a part of the interview, the participants interacted with a functioning 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.

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 and lasted on average 15 minutes. Participants were given a $10 Amazon gift card for participating. 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 asked to discuss 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 other stakeholders. 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.

Finally, we collected participants' demographics at the end of both the phone and in-person interviews.

6.2.3 Data Analysis

We first used an inductive coding process to analyze the in-person interviews. Two researchers independently coded the interviews of five participants and came up with a list of common themes. The researchers then discussed and merged the themes and agreed on a shared codebook with 9 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. The disagreements were tracked, and the inter-coder agreement was measured at 80.6%.

One of the researchers then used the same codebook to code five of the phone interviews. The codebook was then modified to reflect the structure of the phone interviews and discussed by all the authors. The final codebook for the owner interviews emerged with 5 structural codes divided into 15 sub-codes. The researcher used this codebook to code the rest of the phone interviews.

6.3 Results

Our non-owner participants approached the devices with few expectations and learned about the possible features and controls through their interaction with the companion app. Device owners also discussed configuring their devices during initial setup, and rarely revisited most of the controls. Overall, both sets of participants found most of the interface controls usable and understandable. As expected, many of the considerations driving users' explorations related to features of the devices rather than privacy. However, the decisions users make regarding device controls do have implications for what information would be collected, and how it would get used and shared. Thus, we first discuss users' perceptions and privacy implications of the various sets of controls they interacted with or discussed, before further presenting several additional themes that emerged from the study.

6.3.1 Notifications

Notifications are one of the primary means for smart home users to be informed of the device's capabilities and data collection. 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, while notifica-

tions do not necessarily control what information is collected, they are an important awareness mechanism informing users of that collection and providing easy access to the information.

One focus of the interviews was on the different types of controls that customize the delivery of notifications. One way to reduce notifications was to not trigger an event or recording in the first place. For example, all of the participants mentioned tweaking the coverage in front of the smart doorbell to capture the motion only in their desired area. Yet, most of the controls merely customize delivery of the notification, not the recording itself. For example, several of the participants (ON=3, NN=5)[4] mentioned turning off motion notifications when they are having an event in their house or they know that someone will be in front of the doorbell. Participants (ON=2, NN=7) also discussed setting up a schedule for receiving particular 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."

The primary motivation for turning off notifications was to not be bothered by events that participants do not care about. Many of our participants (ON=3, NN=8) wanted notifications only when a delivery happens or a person sets off the motion sensor of the doorbell. Even more so, two of the owner participants wanted notification only when an unknown person triggers the notification. For example, D2

[4]ON: number of owner participants, NN: number of non-owner participants

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."* One owner even turned off motion notification altogether for his 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 users desired to control the field of motion detection for the doorbell camera, for instance, impacting both data collection and notifications. Yet hiding notifications without turning off recording means that users will have reduced awareness of all of the information that is recorded, 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 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.

6.3.2 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 [80]. Many of our novice participants did not directly raise a concern about

this issue from a privacy perspective. Rather, sixteen of the participants talked about the device's storage capacity while interacting with the activity log. They wanted to access the past history of 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.

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 interface. The study interviewers had to provide them with that information when asked. Interestingly, 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 (NN=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."

Participants appreciated their ability to delete the data. However, most of them considered removing the data mostly 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). Even though participants mentioned that it was not important for them to store uneventful recordings (i.e., people coming or going or packages being delivered), participants seldom considered removing such data on their own. Only two owner participants mentioned 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.

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. However, participants also seemed to have expectations that the device manufacturer was storing their data regardless, potentially indefinitely. For instance, D4 mentioned that deleting his information was ineffectual: *"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."*

Yet, this was not always acceptable to participants. For example, five owners would have preferred a way to store data locally. 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."* D4 was 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."* Depending on the device, there are methods for maintaining a local server. However, the complexity of performing this set-up and configuration discouraged the owners from doing so, even though it could give them more control over their data.

In summary, our non-owner participants expressed little or no interest in proactively removing their data when storage is not a concern. Our owner participants seldom erased data on their own. However, the 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.

6.3.3 Video recording

Past research has shown that video and audio are considered as some of the most sensitive data collected by smart home devices [72, 21]. In our study, this only involved the smart doorbell. Most of our participants were comfortable with the audio and video recording capability of the doorbell since the device only records outside of the house. However, some of our participants (NN=8, ON=3) did discuss that the doorbell may record sensitive video/audio or pick up audio from inside the house. 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."

Researchers found similar concerns for smart speakers [53] and indoor security cameras [80]. Our participants reported a range of measures to reduce this concern. Interestingly the owner participants discussed passive approaches by changing their behavior in some way. This included not having a private conversation in front of the device, not sharing the device with anyone, or deleting if a sensitive video gets recorded. In contrast, the novice participants (NN=7) talked about actively turning off the recording for some time (i.e., when kids are playing in the yard) while interacting with the device. 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."* Thus, the ability to easily turn off audio/video recording temporarily is an important feature that may not be sufficiently available in today's doorbells.

Several participants did also discuss their concerns regarding the doorbell's ability to record bystanders. A few of our participants (NN=3, ON=2) 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."*. Owners also mentioned how their doorbell had recorded others: *"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.", D2.

Though concerned, these participants were confused about how bystanders' privacy could be better respected. Interestingly, only the non-owner 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. I don't want every time the neighbor drives in their driveway to pick up by my doorbell.* 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.

Five of our participants (NN=4, ON=1) acknowledged that bystanders could be recorded but 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."

6.3.4 Video sharing

One of the main reasons for using smart doorbells is ensuring the safety of the household. Participants desired to do so by sharing any suspicious videos (i.e., someone stealing packages, house or car break-ins, or randomly roaming around the house) captured by the doorbell with their family and the police. Some of our participants (NN=9, ON=3) wanted to promote the safety of their neighborhood as well, by sharing any suspicious videos with neighbors and neighborhood communities (i.e., Nextdoor, Ring Neighborhood).

Despite these desires to share videos, participants also expressed a range of concerns and behaviors to mitigate those concerns. For example, 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. D6 and D7 also showed concern with sharing video 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."* N5, who has a similar concern, 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."

It was unclear to the participants whether the video link would still be accessible by the public or would be disabled after removing the post from the neighbor app. N17 also 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."*

Bystander privacy came up in the discussion of video sharing as well. Six novice participants mentioned they would 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 on the internet. Moreover, people may make assumptions based on the shared videos. For instance, D6 found videos of a delivery man throwing packages from the car in his neighborhood in the 'neighbor' app. He believed the same person delivered his package, which was broken, and shared that video with the delivery company.

N5 showed his concern for this by saying: *"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?"*

In summary, smart doorbell users are willing to share suspicious videos and random funny videos with their family, friends, police, neighbors, and social media. Yet, participants also sometimes sought out different methods for sharing videos, and had

concerns over the ownership and control of those videos which were not alleviated by the interface.

6.3.5 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. However, many of our participants (NN=12, ON=6) discussed utilizing these features to monitor the bystanders of these devices, especially when the device is shared with 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 participants (NN=4) also mentioned using the devices 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 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 [83].

In addition to monitoring activity, participants also wanted to monitor possible

unauthorized access, especially for the smart lock. Almost half (NN=10) of the non-owner participants mentioned they would want 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 their particular schedule. For instance, N9 mentioned: *"(I want a notification) if someone tried to pull it off the wall to disconnect it, if someone tried to tamper with it or bash it, there should be sensors for that."*

Overall, notifications are the primary means for participants to know about the activities around their devices. Though the non-owner participants appreciated the idea of having the activity log, the owners seldom used it, especially for the smart lock. DL3 mentioned: *"(For the lock) it just shows what events have happened. It is something that you have to look at right away because it's a security hazard."* Instead of regularly checking the whole activity log, participants wanted to look at what they are particularly concerned about (i.e., whether and when kids got home) or when something goes wrong (i.e., someone entered the wrong passcode, error in locking the door). Participants expected advanced filtering mechanisms, for instance, based on the person, time, or errors, to help them with their particular needs.

6.3.6 Access control

Our participants wanted an easy way to share their devices with others, both within and beyond the home. Prior research has highlighted the access control challenges for smart home devices [39, 81], which were also reflected in our results. 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.

The device sharing interfaces of the Ring doorbell and Nest Yale lock led to concerns among 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 participants (NN=8, ON=4) to believe the shared users will have equal access as the owner.

Similar to the findings of Garg et al. [34], and Tabassum et al. [81], the lack of transparency limited users' willingness to share their devices. Both sets of participants decided to share their devices only with close and very trusted people. Our owners were comfortable with their current sharing practices because they mostly shared with the people they trust. And both owners and non-owners were concerned about sharing access with less trusted people (i.e., kids/teenagers, visitors, neighbors, house-sitters, etc.) [39, 81]. For instance, N4 mentioned:

"You would hate for someone else to get in and say, great, we're going to take access away from you. That would be a horrible situation. That is exactly something a middle schooler would do for fun. That would be the time when grandma is sitting outside with two bags of groceries and can't get into the house on a snowy, cold day."

Thus, for less trusted people, participants did not want to add them as shared users. Rather, they prefer providing access via other more limited means, such as a one-time link to view a live stream, remotely opening the lock for a visitor, or sharing codes to access the lock. However, they also recognized that a shared link or

temporary code can 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."*

A few other participants (NN=3, ON=1) 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."* L3 integrated his August lock with Amazon Alexa and appreciated the authentication mechanism when trying to operate 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."* Others also discussed controlling access to shared information, such as N12 who mentioned setting a password to control access to the recorded video in the doorbell.

Participants 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 [81]. Thus they wanted to understand what capabilities and data are being shared in these instances. Specifically, they want 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?"*. Users need transparency and control to not only restrict shared users' access to specific capabilities [39, 81] but also to block them from accessing and downloading particular data points already stored in the device.

Beyond just the 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."*

6.3.7 Emerging themes

Several of additional privacy-related 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, our participants appreciated the remote control and monitoring capabilities of the smart doorbell and lock. However, a few non-owner participants (NN=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."*

Participants exhibited concern using a particular feature when they do not understand how the feature works. 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 (N=19) of our non-owner participants 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, like 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 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 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."*

Similarly, 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 for providing other types of access, which made the process more confusing for our non-owners. 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. DL3, in fact, mentioned that the August lock interface is more informative, as it shows capabilities available to different access levels, and 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.

To summarize, feedback and transparency are critical for making users aware of how the smart devices work, and making them comfortable in utilizing its features. Many of the questions 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, that may reduce their awareness of data collection, leading to undesired privacy risks.

Trust as a prerequisite of purchase: 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 [92]. 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 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 our participants seldom changed the default settings, and only modified specific features to better serve some functional needs (i.e., 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 on interesting reason for this in our interviews. A few participants (NN=3, ON=1) 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."*

Concerns about security: Similar to previous research, we found that participants are concerned about someone hacking their smart devices [88, 80] to intrude upon their homes or information. Our participants (NN=16, ON=3), especially the non-owners, 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 prefer to take other than locking down the lock keypad and relying on the company for the proper security of the lock; however three owner participants changed their behavior to mitigate their concern.

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."* In other words, our owner participants made calculated privacy decisions based on their (lack of) concerns.

Participants were not as concerned about someone hacking the doorbell as the lock, since it did not involve direct access into the house. However, five of the non-owner participants did mention they are concerned of the doorbell being hacked as with any of their internet-connected devices. 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).

6.4 Discussion

Device owners in our study reported configuring their devices and adjusting settings during initial installation. However, our non-owner participants approached this process with few privacy expectations and desires, and instead learned about

the capabilities as they explored the interface. Participants were driven primarily by functional considerations, to achieve their goals for controlling or monitoring their homes. 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. Table 7 summarizes the behaviors seen in our results. Some decisions or desires would serve to increase the collection or access to information, 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 tradeoff 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 usability.

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

(+) Data collection, access and use	(-) 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 7: Behaviors and decisions that increase or decrease data collection, access and use

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 interest to do so.

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 [1].

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 [3].

Yet, defaults are 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. In addition, manufacturers could provide privacy preserving defaults for any settings that require direct end user decisions during installation (i.e., whether the user wants to disable the doorbell from recording audio) and nudge users towards other privacy-related settings on later interactions.

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, i.e., sharing account credentials to provide access. 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.

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 [5].

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 [14]. However, participants also raised a concern that the lack of access control over such features could have unintended consequences.

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.[87] and Cobb et al.[28] 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 nuance access controls and transparency over what accesses are being shared, especially when sharing with less trusted people [81]. However, our study highlighted 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 [2].

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.

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.

6.5 Limitations

We have performed our study with non-owners 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 generalizable 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 department, we did still attract a number of technical participants who likely had deeper understanding of how smart devices operate. However, previous research did not find significant differences in the privacy concerns or behaviors between more knowledgeable and less knowledgeable users [80].

6.6 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.

CHAPTER 7: DISCUSSION, DESIGN GUIDELINES AND CONCLUSION

The overarching goal of this dissertation was to get an in-depth understanding of end-users' perceptions, behaviors, and needs regarding maintaining their data privacy and social privacy in the smart home. In this chapter, I summarize the research contributions of this dissertation by presenting the key findings and the design guidelines. Finally, I conclude by identifying the future works based on this dissertation.

7.1 Summary of result

Smart home users generally understand the wide range of data the devices are collecting and the possibility of using such data to make inferences about their day-to-day lives. However, these perceptions of data practices are mostly formed by the type of device and users' trust relationship with the manufacturers. End-users remain confused about the data practices because of the manufacturer's lack of transparency in privacy notices. Yet, end-users accept trading off some privacy to receive services from these devices. Users also exhibit a lack of concern regarding the data practices of smart home devices. My research identified a number of reasons that contribute to this lack of concern. One such reason is their comfort with the security and privacy practices they employ in the smart home. However, my research shows that participants learned many of these practices from their experience with other computing contexts (i.e., strong passwords, install updates) and primarily rely on manufacturers

for their data and devices' privacy and security. It underscores the importance of providing security and privacy best practices for both users and manufacturers.

Despite users' comfort using the smart home devices, they do have considerations of their privacy in the smart home. My research uncovers several circumstances that lead users to think about their privacy while using smart devices. They employ several practices and behaviors to be more comfortable with their privacy when they have those considerations. For instance, users limit data collection by turning off the microphone in a device. Yet, I found that the devices do not adequately support users in those situations. For instance, controls for limiting data collection are often not easily accessible or readily available to the end-users. As a result, users are often unaware of such privacy controls.

As such, one of the critical issues identified in my research is the challenge of providing awareness to the end-users. Users need to be aware of the data practices, best practices to configure the device, and the available security and privacy controls. I have found end-users expect such awareness to be provided in the app which they use to interact with the device and in the box that comes with the device. Also, my studies indicate that users are more open to receiving such information when they first set up the device. The users can be nudged to more privacy-preserving configurations at the time of the installation. However, one challenge is that providing all this information can be overwhelming for the end-users. Moreover, not all the users are involved in the device installation process, and a third party installs the device in many cases. Furthermore, users often have only one central controller app installed on their mobile phones. It is challenging to provide awareness in such a situation.

Even when users have awareness, I found an inconsistent trust relationship with the manufacturers. As such, users sometimes do not believe the privacy settings offered by the manufacturers. It is not the available controls that provide users assurance of their privacy but their perceptions of the effectiveness of such controls. For instance, users are assured by covering the camera with a physical cap. However, they were not entirely convinced the recordings were removed from the server when deleted from the app. Yet, users trust and rely on the manufacturers for the security and privacy of their data and the device.

Although the trust relationship between the device manufacturers is inconsistent, the relationship between the multiple users of these devices is consistent. Overall, users normally trust their family members with whom they shared the device inside the home. However, I found circumstances that result in users' discomfort even within this trusted environment through unexpected sharing of the information via smart devices. Furthermore, I have noticed the tension between multiple users regarding how these devices should be used. However, most of the time, it is the decision of the primary user (who installs and maintains the device), and it impacts the other users and non-users of the device. For instance, the doorbell camera may record a neighbor's property. I believe primary users should be nudged in some way to consider other stakeholders' opinions and privacy. For instance, the doorbell app can nudge users to block neighbor property from recording.

Another contribution of this dissertation is that it shows end users' sharing behaviors and needs with people outside the house with a complex trust relationship. There are several gaps identified in the current platform regarding end-users' device

sharing needs: 1. lack of fine-grained access sharing control 2. lack of transparency on what access is being shared 3. lack of options to control access to past data when access is shared.

The availability of privacy controls and transparent practices can be proved as a powerful medium for gaining end users' trust. However, the challenge is to provide that to users in a usable way. My research identified that the way such controls are provided has an impact on end-users' security and privacy behavior. Users tend to follow more privacy-preserving behavior when the controls are usable, clearly presented, and meet users' needs (i.e., share the devices via the app instead of sharing the account credentials).

7.2 Design guidelines

Based on the different lessons learned through this dissertation, I propose specific guidelines for manufacturers to enhance the end-user experience of privacy in the smart home.

Data privacy support:

- Provide users with easily accessible controls free of charge to limit data collection and have them available both in the devices and the companion app. These controls should be flexible enough to allow users to configure their devices for different circumstances. For instance, the option to auto-turn on or set a schedule will allow users to turn off data collection for only a specific time without worrying about remembering to turn it on afterward.

- Offer privacy-preserving defaults. Users may not change their default settings.

Hence privacy-invasive features should be turned off by default.

- Develop smart home security and privacy best practices for the users. The device should nudge users to conform to the best practices upon installation.
- Offer options for local storage and processing (inside the device or in the home network) where possible. Nudge users to take security and privacy best practices when choosing this option, for instance to use data encryption.
- Provide a way to access and use data privacy controls and features from the central controller app. The secondary users who only have the central controller app installed should have access to the privacy features.
- Develop smart home security and privacy best practices for the manufacturers. As users primarily depend on the manufacturer for security and privacy, a trusted third party should provide oversight that companies conform to these best practices.

Social privacy support:

- Provide granular access control mechanisms- the ability to provide permission-based, role-based, capability-based, and time-based access. The sharing option should be fine-grained and flexible so users can share the device with different types of people.
- Provide clear and concise information of what features and data are accessible by the shared user. Such information should be provided in the app, specifically in the place where sharing happens.

- Provide features to limit access to historical data, i.e., shared users should only have access to the recordings recorded after it is shared with them.

- Design features to determine how different people are accessing the data and the device. Users should learn how someone uses the device, especially when it is shared with less trusted people.

- Design features and controls to limit unintended sharing of personal data with surroundings, i.e., smart speakers detect if multiple people are present and do not read the notification aloud. Device features should be developed considering the multi-users surrounding.

- Design features to reduce bystanders' data collection, i.e., block out an area from recording in the doorbell. Nudge users to consider bystanders' privacy through device interaction.

Building awareness:

- Provide information about how the device works, data practices, and the available privacy features in the box and the app. Users should be able to review the data practices and privacy settings while they set up the product for the first time.

- Make users aware of a change in privacy setting and inform them of the newly available controls.

- Provide precise information about what major data points the device is collecting in the app.

- Inform users about long-unused features that result in data collection. Users may forget about activating a feature, and it may result in a negative user experience when they become aware of the unnecessary data collection.

- Alert users to reset the device in the cases of device re-use. The device may contain sensitive data of the previous owner, and re-using the device would provide the new users un-intended access to that data.

- Provide a visible indicator both in the device and the app to indicate data collection. These indicators should be carefully designed as users may get confused if similar indicators are used for different purposes.

- Design an 'out of the box' solution to provide the above-mentioned awareness to the secondary users of the devices who are not involved with the installation process and often do not have the companion app installed in their mobile phones.

- Provide specific information about what is updating when an update occurs. Offer users options to access the updated settings, where applicable.

Building trust:

- Be more transparent about security and privacy practices. Notices should be brief, focusing on practices that end-users most care about and may find surprising.

- Build open-source systems to allow a broad community of users and researchers to identify practices.

- Provide support for troubleshooting, for instance, in case of device malfunction.
- Offer FAQ, help & support features in the app and in the online account.

7.3 Future Work

This research presents one key insight that the available privacy features often do not meet the end-users' needs. It also shows the need for fine-grained control regarding data and access control. Yet, there is limited research on how smart home devices make privacy design choices in the smart home and conform to these needs. Future research should evaluate the features (or lack thereof) designed to enhance users' awareness and privacy in different types of commercially available smart home devices to identify the gap between users' needs and available controls.

In addition to that, my study uncovers the complexity of providing access to privacy-related information and controls to secondary users. It also provides specific guidelines to improve awareness, such as providing awareness and control in the central controller app. More research is needed to be done specifically on secondary users to understand their needs and interaction dynamics with the device to identify opportunities to provide them awareness and control. Moreover, I believe future research should look particularly at households where a highly technically skilled primary user customizes their smart home using advanced mechanisms such as writing scripts. The secondary users' role, behavior, and need in such a household, especially in the absence of the primary user, is still lacking in the literature.

Another interesting issue I found is the increasing involvement of third parties in the device installation and setup process. Research is needed to understand these

new dynamics, especially how end-users become aware of the features available in the device and who bears the responsibility of security and privacy of the device in such a household. Finally, my studies shed light on how smart home devices impact bystanders' privacy. More research should be done to determine how the considerations of the bystanders can be integrated into the device settings and how to provide them notice of data collection. However, giving transparency to bystanders may have consequences on the owners' security and privacy. For instance, providing notice of camera recording in a door placard may allow a malicious party to cut the fiber cable and disable the camera. Hence, research is needed to investigate how to balance transparency and privacy such that awareness features are effective for the end-users.

7.4 Conclusion

The adoption and use of smart home devices are growing exponentially. However, the ubiquitous and pervasive data collection capabilities allow these devices to inconspicuously collect a vast amount of data resulting in end users' security and privacy concerns. Research in other computing contexts shows that end-users' concerns may be lessened by providing them with more awareness and control over the device and data. It is imperative to understand the end-user perspective of security and privacy to design these mechanisms effectively.

In this dissertation, I have investigated different aspects of privacy that end-users experience in the smart home, i.e., data privacy and social privacy. I contributed to the state of the art by providing a deep understanding of what these different as-

pects of privacy mean for smart home users, their salient privacy concerns, behaviors, and needs. Moreover, I expanded the previous research by presenting end-users' in-situ privacy considerations and several circumstances eliciting those considerations. Furthermore, my research increases the understanding of how end-users utilize the available features to manage their privacy considerations and how such mechanisms impact their privacy behaviors. Finally, drawing from these findings, I have synthesized a number of design guidelines for smart home researchers and manufacturers to increase end-user trust, privacy awareness, and control over their data and social privacy. I hope this dissertation will pave the way for a more privacy-preserving and secure smart home ecosystem respecting all the stakeholders (primary users, secondary users, and bystanders).

REFERENCES

[1] Alexa for business faqs. https://aws.amazon.com/alexaforbusiness/faqs/. Accessed: 2021-09-07.

[2] Allowing access to shared users and controlling ring devices with multiple electronic devices. https://bit.ly/3qVlIc1. Accessed: 2021-09-07.

[3] Amazon wants smart home device setup to be a 'zero-touch' experience. https://venturebeat.com/2019/07/05/amazon-wants-smart-home-device-setup-to-be-a-zero-touch-experience/. Accessed: 2021-09-07.

[4] Bob evans, 2014. https://pacoapp.com/. Accessed: 2022-21-01.

[5] Default settings for privacy – we need to talk. https://www.cnet.com/news/default-settings-for-privacy-we-need-to-talk/. Accessed: 2021-09-07.

[6] The facebook and cambridge analytica scandal, explained with a simple diagram. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram. Accessed: 2019-11-26.

[7] Hackers can hijack wi-fi hello barbie to spy on your children. https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children. Accessed: 2019-11-26.

[8] Home assistant adopter beware: Google, amazon digital assistant patents reveal plans for mass snooping. https://bit.ly/346krpz. Accessed: 2019-11-26.

[9] House votes to allow internet service providers to sell, share your personal information. https://bit.ly/3rFnmxO. Accessed: 2019-11-26.

[10] Mozilla - *privacy not included. https://foundation.mozilla.org/en/privacynotincluded/. Accessed: 2019-02-13.

[11] Project alias. http://bjoernkarmann.dk/project_alias. Accessed: 2019-02-13.

[12] Smart devices leaking data to tech giants raises new iot privacy issues. https://bit.ly/3tWgtLp. Accessed: 2019-11-26.

[13] Statista smart home report. https://www.statista.com/outlook/279/109/smart-home/united-states. Accessed: 2019-11-26.

[14] Using accessibility features on echo devices with a screen. https://www.amazon.com/gp/help/customer/display.html?nodeId=202158200. Accessed: 2021-09-07.

[15] Why homes with a 6-metre driveway get cheaper insurance: From supermarket loyalty cards to google maps - the secret data firms use to set your premiums. `https://www.thisismoney.co.uk/money/bills/article-2749831/The-secret-data-firms-use-set-premiums.html`. Accessed: 2019-11-26.

[16] N. Abdi, X. Zhan, K. M. Ramokapane, and J. Such. Privacy norms for smart home personal assistants. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2021.

[17] M. S. Ackerman, L. F. Cranor, and J. Reagle. Privacy in e-commerce: Examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce*, EC '99, pages 1–8, New York, NY, USA, 1999. ACM.

[18] N. Aleisa and K. Renaud. Yes, I know this IoT device might invade my privacy, but I love it anyway! a study of Saudi Arabian perceptions. In *2nd International Conference on Internet of Things: Big Data and Security (IoTBDS 2017)*, pages 198–205, 2017.

[19] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. 08 2017.

[20] N. Apthorpe, Y. Shvartzshnaider, A. Mathur, D. Reisman, and N. Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(2):59:1–59:23, July 2018.

[21] N. Apthorpe, Y. Shvartzshnaider, A. Mathur, D. Reisman, and N. Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):1–23, 2018.

[22] N. M. Barbosa, J. S. Park, Y. Yao, and Y. Wang. " what if?" predicting individual users' smart home privacy preferences and their changes. *PoPETs*, 2019(4):211–231, 2019.

[23] A. Brush, J. Jung, R. Mahajan, and F. Martinez. Digital neighborhood watch: Investigating the sharing of camera data amongst neighbors. In *Proceedings of the 2013 conference on Computer supported cooperative work*, pages 693–700. ACM, 2013.

[24] A. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon. Home automation in the wild: Challenges and opportunities. ACM Conference on Computer-Human Interaction, May 2011.

[25] A. B. Brush and K. M. Inkpen. Yours, mine and ours? sharing and use of technology in domestic environments. In *International Conference on Ubiquitous Computing*, pages 109–126. Springer, 2007.

[26] E. K. Choe, S. Consolvo, J. Jung, B. Harrison, S. N. Patel, and J. A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp '12, pages 61–70, New York, NY, USA, 2012. ACM.

[27] J. W. Clark, P. Snyder, D. McCoy, and C. Kanich. "i saw images i didn't even know i had": Understanding user perceptions of cloud storage privacy. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 1641–1644, New York, NY, USA, 2015. ACM.

[28] C. Cobb, S. Bhagavatula, K. A. Garrett, A. Hoffman, V. Rao, and L. Bauer. "i would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies*, 4:54–75, 2021.

[29] A. Das, M. Degeling, D. Smullen, and N. Sadeh. Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3):35–46, Jul 2018.

[30] A. Das, M. Degeling, X. Wang, J. Wang, N. Sadeh, and M. Satyanarayanan. Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, pages 1387–1396. IEEE, July 2017.

[31] C. Dixon, R. Mahajan, S. Agarwal, A. Brush, B. Lee, S. Saroiu, and P. Bahl. An operating system for the home. In *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*, pages 25–25. USENIX Association, 2012.

[32] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 447–464. IEEE, 2020.

[33] Y. Feng, Y. Yao, and N. Sadeh. 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*, CHI '21, page 1–16, New York, NY, USA, 2021. Association for Computing Machinery.

[34] R. Garg and C. Moreno. Understanding motivators, constraints, and practices of sharing internet of things. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 3(2):44:1–44:21, June 2019.

[35] C. Geeng and F. Roesner. Who's in control?: Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 268:1–268:13, New York, NY, USA, 2019. ACM.

[36] C. Geeng and F. Roesner. Who's in control?: Interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, page 268. ACM, 2019.

[37] M. Ghiglieri, M. Volkamer, and K. Renaud. Exploring consumers' attitudes of smart TV related privacy risks. In T. Tryfonas, editor, *Proceedings of the 5th International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS)*, Lecture Notes in Computer Science, pages 656–674, Cham, 2017. Springer.

[38] J. Haney, Y. Acar, and S. Furman. " 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)*, 2021.

[39] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur. Rethinking access control and authentication for the home internet of things (iot). In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 255–272, 2018.

[40] G. N. Help. Learn about family accounts and how to share access to your nest home. `https://support.google.com/googlenest/answer/9304271?co=GENIE.Platform%3DAndroid&hl=en`. Accessed: 2019-09-20.

[41] R. Help. Controlling ring devices through multiple devices or sharing control with other users. `https://support.ring.com/hc/en-us/articles/211018223-Controlling-Ring-Devices-through-Multiple-\Devices-or-Sharing-Control-with-Other-Users`. Accessed: 2019-09-20.

[42] C. Horne, B. Darras, E. Bean, A. Srivastava, and S. Frickel. Privacy, technology, and norms: The case of smart meters. *Social Science Research*, 51:64 – 76, 2015.

[43] Y. Huang, B. Obada-Obieh, and K. K. Beznosov. Amazon vs. my brother: How users of shared smart speakers perceive and cope with privacy risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[44] M. Johnson and F. Stajano. Usability of security management: Defining the permissions of guests. In *International Workshop on Security Protocols*, pages 276–283. Springer, 2006.

[45] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, 2015. USENIX Association.

[46] Z. Kaupas and J. Ceponis. End-user license agreement-threat to information security: a real life experiment. In *Proceedings of the IVUS International Conference on Information Technology*, pages 55–60, 2017.

[47] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. Challenges in access right assignment for secure home networks. In *HotSec*, 2010.

[48] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker. Access right assignment mechanisms for secure home networks. *Journal of Communications and Networks*, 13(2):175–186, 2011.

[49] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall. "when i am on wi-fi, i am fearless": Privacy concerns & practices in eeryday wi-fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pages 1993–2002, New York, NY, USA, 2009. ACM.

[50] V. Koshy, J. S. S. Park, T.-C. Cheng, and K. Karahalios. "we just use what they give us": Understanding passenger user perspectives in smart homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2021.

[51] K. Kostiainen, O. Rantapuska, S. Moloney, V. Roto, U. Holmstrom, and K. Karvonen. Usable access control inside home networks. In *2007 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pages 1–6. IEEE, 2007.

[52] J. Lau, B. Zimmerman, and F. Schaub. "alexa, stop recording": Mismatches between smart speaker privacy controls and user needs. `https://www.usenix.org/sites/default/files/soups2018posters-lau.pdf`. Accessed: 2018-09-10.

[53] J. Lau, B. Zimmerman, and F. Schaub. Alexa, are you listening?: Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW):102:1–102:31, Nov. 2018.

[54] S. Lederer, J. Mankoff, and A. K. Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '03, pages 724–725, New York, NY, USA, 2003. ACM.

[55] H. Lee and A. Kobsa. Understanding user privacy in internet of things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412, Dec 2016.

[56] L. Lee, J. H. Lee, S. Egelman, and D. Wagner. Information disclosure concerns in the age of wearable computing. In *Proceedings of the NDSS Workshop on Usable Security (USEC '16)*. Internet Society, 2016.

[57] R. Leitão. Anticipating smart home security and privacy threats with survivors of intimate partner abuse. *Proceedings of the 2019 on Designing Interactive Systems Conference*, 2019.

[58] V. Lekakis, Y. Basagalar, and P. Keleher. Don't trust your roommate or access control and replication protocols in "home" environments. In *In Proc. HotStorage*. Citeseer, 2012.

[59] N. Malkin, J. Bernd, M. Johnson, and S. Egelman. "what can't data be used for?" privacy expectations about smart tvs in the us. In *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC)*.

[60] N. Malkin, J. Deatrick, A. Tong, P. Wijesekera, S. Egelman, and D. Wagner. Privacy attitudes of smart speaker users. *PoPETs*, 2019:250–271, 2019.

[61] S. Mare, L. Girvin, F. Roesner, and T. Kohno. 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*, HotMobile '19, pages 117–122, New York, NY, USA, 2019. ACM.

[62] S. Mare, F. Roesner, and T. Kohno. Smart devices in airbnbs: Considering privacy and security for both guests and hosts. *Proceedings on Privacy Enhancing Technologies*, 2020(2):436–458, 2020.

[63] T. Maronick. Do consumers read terms of service agreements when installing software?a two-study empirical analysis. *International Journal of Business and Social Research*, 4(6), 2014.

[64] R. Marvin. Privacy tops list of consumer smart home concerns. `https://www.pcmag.com/news/366783/privacy-tops-list-of-consumer-smart-home-concerns`. Accessed: 2019-11-26.

[65] M. L. Mazurek, J. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, et al. Access control for home data sharing: Attitudes, needs and practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 645–654. ACM, 2010.

[66] D. McKay and C. Miller. 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*, pages 1–14, 2021.

[67] A. McStay. Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy). *Big Data & Society*, 3(2), 2016.

[68] S. Mennicken, D. Kim, and E. M. Huang. Integrating the smart home into the digital calendar. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 5958–5969, New York, NY, USA, 2016. ACM.

[69] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma. Iot sentinel: Automated device-type identification for security enforcement in iot. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 2177–2184. IEEE, 2017.

[70] A. Montanari, A. Mashhadi, A. Mathur, and F. Kawsar. Understanding the privacy design space for personal connected objects. In *Proceedings of the 30th British Human Computer Interaction Conference (British HCI 2016)*, 07 2016.

[71] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh. Privacy expectations and preferences in an iot world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, Santa Clara, CA, 2017. USENIX Association.

[72] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh. Privacy expectations and preferences in an iot world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 399–412, 2017.

[73] S. R. Peppet. Regulating the internet of things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review*, 93:85–179, 11 2014.

[74] D. Randall. Living inside a smart home: A case study. In *Inside the smart home*, pages 227–246. Springer, 2003.

[75] Ring. Ring neighborhood watch. `https://shop.ring.com/pages/neighbors`. Accessed: 2019-09-20.

[76] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons. Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. 10 2015.

[77] S. Schechter. The user is the enemy, and (s)he keeps reaching for that bright shiny power button! In *Proceedings of the Workshop on Home Usable Privacy and Security (HUPS)*, July 2013.

[78] A. K. Simpson, F. Roesner, and T. Kohno. Securing vulnerable home iot devices with an in-hub security manager. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 551–556, March 2017.

[79] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani. Network-level security and privacy control for smart-home iot devices. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 163–167, Oct 2015.

[80] M. Tabassum, T. Kosinski, and H. R. Lipford. "i don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth*

Symposium on Usable Privacy and Security (SOUPS 2019), Santa Clara, CA, Aug. 2019. USENIX Association.

[81] M. Tabassum, J. Kropczynski, P. Wisniewski, and H. R. Lipford. 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*, CHI '20, page 1–12, New York, NY, USA, 2020. Association for Computing Machinery.

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

[83] B. Ur, J. Jung, and S. Schechter. 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*, pages 129–139. ACM, 2014.

[84] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 11:1–11:16, New York, NY, USA, 2010. ACM.

[85] P. Worthy, B. Matthews, and S. Viller. Trust me: Doubts and concerns living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS '16)*, pages 427–434, New York, 2016. ACM.

[86] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang. 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*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[87] Y. Yao, J. R. Basdeo, O. R. Mcdonough, and Y. Wang. Privacy perceptions and designs of bystanders in smart homes. 3(CSCW), Nov. 2019.

[88] E. Zeng, S. Mare, and F. Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, Santa Clara, CA, 2017. USENIX Association.

[89] E. Zeng, S. Mare, and F. Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 65–80, 2017.

[90] E. Zeng and F. Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 159–176, 2019.

[91] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):200, 2018.

[92] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster. User perceptions of smart home iot privacy. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW):200:1–200:20, Nov. 2018.

[93] V. Zimmermann, M. Bennighof, M. Edel, O. Hofmann, J. Jung, and M. von Wick. 'home, smart home' - exploring end users' mental models of smart homes. In R. Dachselt and G. Weber, editors, *Mensch and Computer 2018 - Workshopband*, Bonn, 2018. Gesellschaft für Informatik e.V.