Smart Home Beyond the Home: A Case for Community-Based Access Control

Madiha Tabassum[1], **Jess Kropczynski**[2], **Pamela Wisniewski**[3], **Heather Richter Lipford**[1]
University of North Carolina at Charlotte[1], University of Cincinnati[2], University of Central Florida[3]
[mtabassu, Heather.Lipford]@uncc.edu, jess.kropczynski@uc.edu, pamwis@ucf.edu

ABSTRACT
As smart devices are becoming commonplace in homes, we need to explore the needs of not just the residents of the home, but also of secondary stakeholders who may be granted access to these devices from outside of the home. We conducted a mixed methods study, which included a survey of 163 smart home device owners and a follow-up interview with 13 individuals who currently share their smart home devices with others outside of their home. Nearly half (47.8%) of our survey participants shared at least one smart home device with someone that did not live with them. Individuals sought greater safety and security by providing remote access to trusted family members or friends. By understanding users' perspectives about privacy and trust in relation to sharing smart home devices beyond the home, we build a case for community-based access control of smart home devices in the Internet of Things.

Author Keywords
Community; Access Control; Smart home

CCS Concepts
•**Human-centered computing** → **Empirical studies in collaborative and social computing;** •**Security and privacy** → *Human and societal aspects of security and privacy;*

INTRODUCTION
Smart home devices are being rapidly adopted throughout the world. There were nearly 45 million smart home devices installed in the US alone at the end of 2018 [1], with nearly 20% of American consumers having access to a smart speaker [2]. As the number of households that contain smart devices proliferate, users will become increasingly reliant on such devices for home automation, safety, and convenience. Typically, the setup and administration of these devices is done by a single person, yet the use and care of our homes rarely involves just one person. Multiple people may live in a home, family and friends visit, house cleaners and contractors help with maintenance, and neighbors keep an eye out for emergencies. In other words, there are potentially many people who have a stake in the well-being of the home and its occupants, and each may benefit from the affordances of smart home devices. There is still limited research examining how smart home devices can be used and shared amongst this community of people. We aim to address this gap in our research.

In this paper we focus in particular on secondary stakeholders: people who do not live in the home. We also focus on remote usage of smart home devices. Remote access to a smart home is one of the primary benefits of these 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 [3, 4]. Friends or family members could remotely check on pets, or let in people delivering packages, should the homeowner not be available. We seek to understand the range of potential uses for this remote sharing, as well as the needs for homeowners to monitor and control such access.

We present the results of 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?

We were surprised to discover that nearly half of our survey participants reported that they already do share remote access to their smart home devices with people who do not live in their homes, and another 17% desire such sharing. Our results provide detailed information regarding who, what, and why these devices are shared. We conducted follow-up interviews with 13 people who already share their smart home devices, further exploring their motivations, behaviors, and needs. Our results provide the following contributions:

CHI '20, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
http://dx.doi.org/10.1145/3313831.3376255

- We identify the needs of remotely sharing smart home devices with a trusted set of close friends and family.
- We characterize the current and desired practices for remote sharing of smart home devices to enable collective care and monitoring of a home and its occupants.
- We argue that smart home device designers should examine community-based models of device usage and sharing to identify additional needs and solutions around access control of smart home devices.

RELATED WORK

We begin by discussing research that examines community-oriented security and privacy management, then work specifically examining access control for multi-user smart homes.

Privacy beyond the individual

While much of the privacy and security literature focuses on individual decision-making and behaviors, we turn our attention to a subset of that literature that engages groups and communities in discussion and management of privacy and security. In the physical world, there are many examples of how community structures strengthen security and safety, most notably, neighborhood watch groups[5, 6].These groups help to provide social infrastructure to inspire collective action among neighbors through regular in-person meetings [5]. In considering the social infrastructure that supports oversight mechanisms for neighborhood watch, we wonder how software and access control models for devices in the Internet of Things can increase participation in privacy and security management beyond the individual.

This social infrastructure of IoT devices is largely unexplored territory due to limitations of the software itself. However, the evolution of Web 2.0 [7], has shown that access to tools for creation, collaboration, and sharing can unlock new community building potential. Previous studies have utilized communication privacy management theory (CPM) to better understand the way people make decisions to reveal or conceal private information on social networking sites, and found that understanding group privacy is an important consideration in evolving privacy management strategies [8]. Understanding tradeoffs as they apply to specific smart home devices and use cases [9, 10] is important to the design of social infrastructure to support IoT device sharing.

Microsoft Research explored the digitization of the traditional neighborhood watch using shared security camera data [4]. Participant interviews revealed that although privacy concerns were raised, this could be alleviated by aiming cameras at the foreground or sidewalks in front of a home. Today, industry has implemented this type of capability, such as with the Ring Neighbor's App that provides real time sharing and alerts [3]. Page et al. found that many users have a community-oriented view of IoT devices, where those devices facilitate interactions between multiple people and objects, resulting in potential benefits as well as privacy concerns that go beyond an individual[11]. Thus, in this paper we examine this viewpoint, and the benefits and concerns that could arise when devices are used within trusted communities of people.

Smart home access control

People, in general, have complex access control preferences for sharing digital devices in their homes [12, 13, 14]. While residents may trust each other, prior research has found that they also prefer to keep separate profiles in their digital devices [12] and often try to implement complicated policies using makeshift methods, especially when their mental model of access control is misaligned with the actual system [13].

However, with the advancement of technology, smart home devices can now collect and analyze more (and more sensitive) data within homes, relay all of this information to users, all to enhance the potential for managing different domestic systems (e.g., heating, lighting, entertainment) [15]. However, with the benefits also comes the need for more flexible as well as rigorous access control policies as these privacy-sensitive smart devices often get shared among multiple stakeholders (i.e., roommates [14], guests [16], neighbors [4], teenagers [17], and kids [18]) with different trust and social relationships. 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 [19]. 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 [20].

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 [21, 22]. 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 [23]. Rendall et al. however pointed out that as control systems become more complicated, people feel they actually have less control over their devices [24]. 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 [25].

Though these initial studies looked at different aspects of smart home access-control, both the consumer landscape and devices have changed significantly in recent years. Most smart home 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 [26]. The Nest thermostat gives users an option to add a family member, providing them full access to the device [27]. 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 [28, 9]. In a large scale vignette study, He et al. [29] 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.[30] 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.

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 [19], 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. Thus, we add to the understanding of smart home device sharing and access control by focusing on usage of the smart home by those who are not located and do not live within the home.

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. The complete interview and survey questions are provided in the supplemental materials. All methods were approved by our university IRBs.

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 (for details, see the survey in the supplemental materials). 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 the remote access of 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[1]. 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.

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. The full set of questions is in the supplemental materials.

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.

[1] If participants only owned two devices (minimum criteria for participating) then they were only asked about those two.

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.

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.

SURVEY RESULTS

We begin by providing an overview of our survey participants, then present the details of their current and desired sharing decisions, followed by the reasons behind and the elements affecting those decisions.

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.

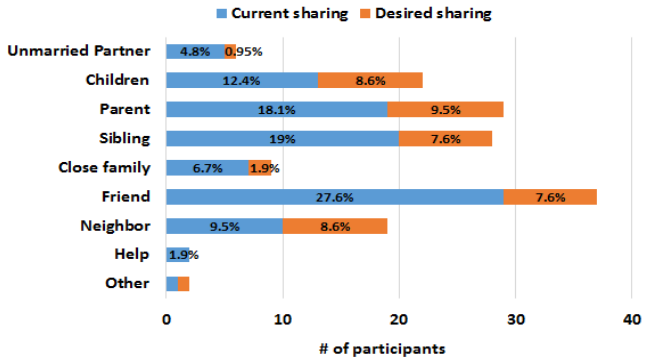

Figure 1. Who do participants share their devices with?

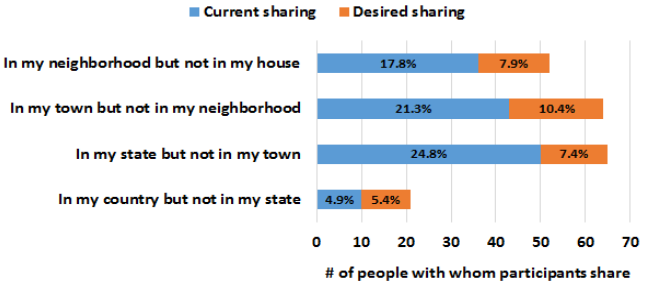

Figure 2. Where do the people live?

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.

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.

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.1).

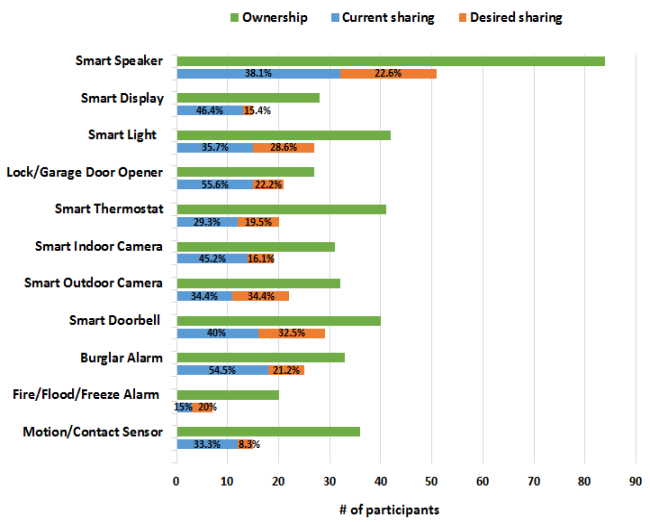

Figure 3. Which devices do participants share outside of the home?

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. 2). 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.

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 3). 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 the participants), and smart doorbells (72.5%). Smart indoor (61.39%) and outdoor cameras (68.8%) 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 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 home". We ask this question for at most three devices for each person the participant mentioned[2]. Hence, the percentages for each capability were 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 4, with the remaining graphs found in the supplemental materials.

We found that for smart cameras and doorbells, the most frequently shared capabilities are viewing live streaming (shared

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

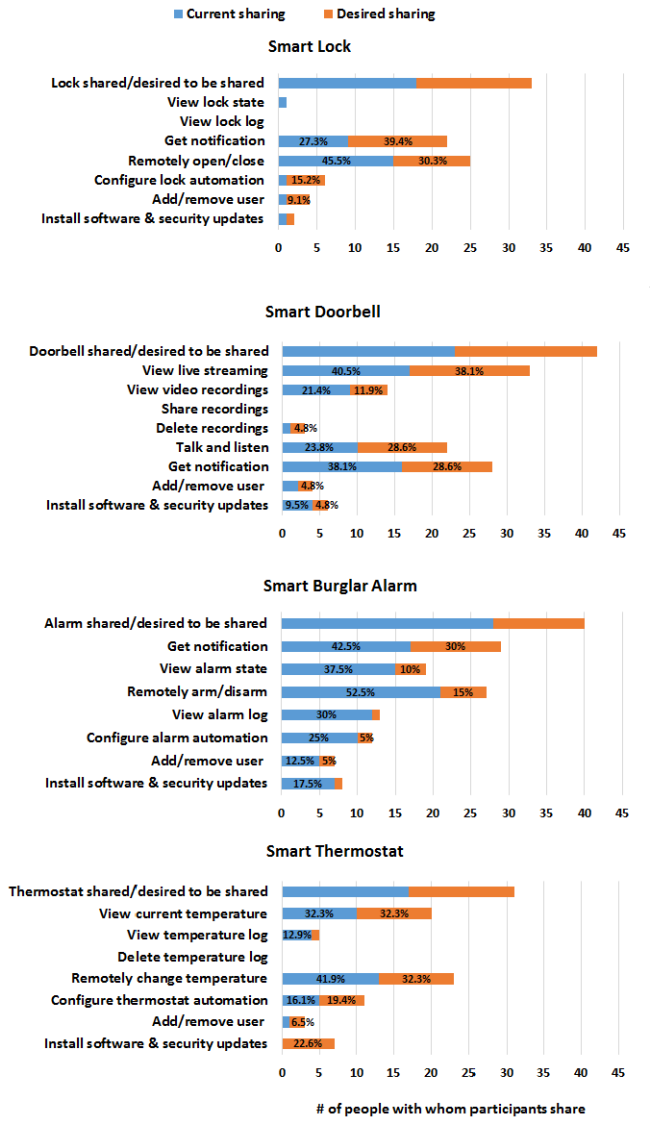

Figure 4. Which capabilities do participants share?

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 smart burglar alarms (with 72.5% people), fire/freeze alarms (with 80% 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 light and, 74.2% people for thermostat) and smart speakers (with 58.7% 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 to pick 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.

Reciprocal sharing

To learn more about how smart homeowners perceive device sharing relationships 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[3]. 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.

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 elements affecting participants' smart home device sharing decisions [4].

Benefits received from sharing the devices

The perceived benefit was the driving motivation 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 individual 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 pets and people in 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 (36.8%) 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 element 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

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

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

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?" 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 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."*

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 elements 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.

Participant profiles

Our interviewees consisted of 9 males and 4 females 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 renters. The descriptive statistics of our participants are summarised in Table 1, 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 year 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 username and password 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 year 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. These participants mentioned sharing the devices would help when they travel somewhere without any Internet access, or because they simply prefer to have a backup person who can remotely monitor their house.

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."* Thus, while we cannot confirm a correlative relationship between location and sharing decisions in our survey study, proximity anecdotally emerged as a consideration for some individuals. Still, participants also share with people not in close proximity. Eric and Ben share their alarms with family members who live far away, but who can still help notify appropriate people in case of a break-in or fire.

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

Table 1. Summary of interview participants. * indicates the devices currently shared by the participants.

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.

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.

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: *"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 full 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.

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.*

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.Some interview participants mentioned providing access to devices such as locks and lights when someone visits their home, they also stated specific reasons for wanting to grant remote access for these same trusted people. Participants chose to share with people they 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 [4].

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. While past research has found nuanced access control needs for different kinds of people within and outside of a home, our results also show the needs for smart home device designers to examine community-oriented models and needs of sharing remote access to homes and devices.

Unlike prior research which identified nuanced access control desires for different audiences [29, 30], 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 [22, 25, 30, 29], users do need methods to allow for more restricted forms of sharing, to enable the expansion of the community which they can rely on to help them with their homes. However, access control may differ for remote users. For instance, past research emphasizes that people want to control access inside the home based on the location of the secondary stakeholder and whether they were around when the access was granted [29]. However, our results suggest that designers should explore more time- or event-based access controls to support remote monitoring and notification needs. Additionally, within-home roles, such as admin, child, and visitor [19] will also differ, driven by the use cases we have identified in this paper. Hence, explicit features to add people outside of the home would be the first step towards addressing users' needs. 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.

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 users who are reluctant to share their smart home devices with people outside of their house.

CONCLUSION AND FUTURE WORK

In conclusion, our study demonstrates that smart device owners are taking a community-oriented approach to the safety and care of their homes. 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. Based on our results, we plan to design and prototype new control mechanisms to improve the capabilities of smart home sharing beyond the home to meet the needs we have identified here. Future work in this area should continue to focus on community-based designs that support the variety of users and stakeholders of smart home IoT devices.

ACKNOWLEDGMENTS

This research was supported by the U.S. National Science Foundation under grants CNS-1814068, CNS-1814110, and CNS-1814439 and a 2018H1 Mozilla Research Grant. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

REFERENCES

[1] Michael Caccavale. The impact of the digital revolution on the smart home industry. http://bit.ly/2MY6FKy. Accessed: 2019-09-20.

[2] Sarah Perez. 47.3 million u.s. adults have access to a smart speaker, report says. https://tcrn.ch/2MSx2S8. Accessed: 2019-09-20.

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

[4] AJ Brush, Jaeyeon Jung, Ratul Mahajan, and Frank 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.

[5] James Garofalo and Maureen McLeod. The structure and operations of neighborhood watch programs in the united states. *Crime & Delinquency*, 35(3):326–344, 1989.

[6] Dennis P Rosenbaum. The theory and research behind neighborhood watch: Is it a sound fear and crime reduction strategy? *Crime & Delinquency*, 33(1):103–134, 1987.

[7] Tim O'reilly. What is web 2.0: Design patterns and business models for the next generation of software. *Communications & strategies*, (1):17, 2007.

[8] Ralf De Wolf, Koen Willaert, and Jo Pierson. Managing privacy boundaries together: Exploring individual and group privacy management strategies in facebook. *Computers in Human Behavior*, 35:444–454, 2014.

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

[10] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):200, 2018.

[11] Xinru Page, Paritosh Bahirat, Muhammad Safi, Bart Knijnenburg, and Pamela Wisniewski. The internet of what?: Understanding differences in perceptions and adoption for the internet of things. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2:1–22, 12 2018.

[12] AJ Bernheim Brush and Kori 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.

[13] Michelle L Mazurek, JP Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon 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.

[14] Vassilios Lekakis, Yunus Basagalar, and Pete Keleher. Don't trust your roommate or access control and replication protocols in "home" environments. In *In Proc. HotStorage*. Citeseer, 2012.

[15] Steven K Firth, Farid Fouchal, Tom Kane, Vanda Dimitriou, and Tarek M Hassan. Decision support systems for domestic retrofit provision using smart home data streams. CIB, 2013.

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

[17] Blase Ur, Jaeyeon Jung, and Stuart 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.

[18] Stuart 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.

[19] A.J. Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. Home automation in the wild: Challenges and opportunities. ACM Conference on Computer-Human Interaction, May 2011.

[20] Colin Dixon, Ratul Mahajan, Sharad Agarwal, AJ Brush, Bongshin Lee, Stefan Saroiu, and Paramvir 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.

[21] Tiffany Hyun-Jin Kim, Lujo Bauer, James Newsome, Adrian Perrig, and Jesse Walker. Challenges in access right assignment for secure home networks. In *HotSec*, 2010.

[22] Tiffany Hyun-Jin Kim, Lujo Bauer, James Newsome, Adrian Perrig, and Jesse Walker. Access right assignment mechanisms for secure home networks. *Journal of Communications and Networks*, 13(2):175–186, 2011.

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

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

[25] Kari Kostiainen, Olli Rantapuska, Seamus Moloney, Virpi Roto, Ursula Holmstrom, and Kristiina 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.

[26] Ring Help. Controlling ring devices through multiple devices or sharing control with other users. http://bit.ly/39NC24f. Accessed: 2019-09-20.

[27] Google Nest 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.

[28] Christine Geeng and Franziska 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.

[29] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase 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.

[30] Eric Zeng and Franziska 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.