Exploring Smart Home Device Sharing Beyond the Home

| Anonymized  For  Peer  Review |
| --- |

# ABSTRACT

Paste the appropriate copyright/license statement here. ACM now supports three different publication options:

* ACM copyright: ACM holds the copyright on the work. This is the historical approach.
* License: The author(s) retain copyright, but ACM receives an exclusive publication license.
* Open Access: The author(s) wish to pay for the work to be open access. The additional fee must be paid to ACM.

This text field is large enough to hold the appropriate release statement assuming it is single-spaced in Times New Roman 8-point font. Please do not change or modify the size of this text box.

Each submission will be assigned a DOI string to be included here.

Understanding a user’s needs and use cases for which they might find value in a technology are pivotal to success of any technology. We conducted a web-based pilot survey with nineteen smart home users to gain insights into their thoughts on sharing their smart home devices with people outside their home. We aimed to find why and with whom, if at all, the users would like to share which particular devices. We also studied their motivation and the factors which affect their decision. We found that most people preferred to share their smart camera, security system and locks with family members and friends to allow them to access their home for emergencies when they are not home and to monitor and take care of their property. Our findings provide new insights into the end user’s perspective on sharing of smart home devices outside of home and help formulate design-specific recommendations for such systems.

## Author Keywords

Smart Device; Internet-of-Things; Smart Home; Access Control; IoT Sharing;

## ACM Classification Keywords

# K.4.0 General

# INTRODUCTION

Smart devices in households are being employed for applications ranging from home security, automation and control to entertainment, energy management and comfort. A “smart” device can be said to be a device that is computer networked, user reconfigurable and that can operate autonomously to some extent [20]. Internet connected smart devices have led to a phenomenon called Internet of Things (IoT) [13,23] which is an application domain that integrates different technological and social fields. [17]. Number of devices connected to the internet have already surpassed number of humans in the world and IoT devices are following suit [21,26]. With more homes getting connected to the Internet, “smart” devices are also becoming increasingly popular in households [27]. For example, twenty percent of US Wi-Fi households have a smart speaker in 2018 [28]. This demonstrates the rapid adoption of smart speakers which are fairly new in the market with the two primary market share holders Amazon and Google first releasing their smart speakers in July 2015 and November 2016 respectively [25,29,30]. The rapid adoption of smart cameras and smart doorbells is another testament to the explosive adoption on Home IoT. Networking hardware company Cisco projects that nearly three-quarters of devices connected to the internet will be smart devices by 2021 [31].

With the ability of accessing smart home devices remotely from the Internet comes the ability of sharing this access with others. New trends are evolving in sharing smart home devices to interconnect people, such as the Ring neighborhood system [32]. For example, a suspicious person or event captured by a smart doorbell may be useful for the neighbors so that they can be aware and possibly help making the neighborhood safer. Neighbors with access to smart home alarm can be quick to respond to alarms like burglar, fire or flood alarms. A neighbor with access to a smart lock can let it emergency responders when you are not home and even call off false alarms to prevent unnecessary police or fire dispatch which may carry heavy penalties. Since smart home devices are connected to the Internet, it is possible to access the device and its’ data from anywhere in the world. This very design gives smart devices the implicit property of possibly being shared over the Internet with anybody. To expand the body of knowledge and to identify possible design improvements for the existing state of smart home device sharing technology, we set out to understand the users’ needs and perceptions surrounding this topic. We posed the following high-level research questions:

* **RQ1:** Are smart home users willing to share access to their smart home devices with people outside their homes? Which smart home devices are users willing to share and for what purpose?
* **RQ2:** With whom are smart home users willing to share access to their smart devices and how personal relationships and distance affect their decision?

To address these questions, we conducted a mixed qualitative and quantitative survey of 19 smart home users. The survey was conducted online and required that the participants own at least one smart home device. We analyzed what is important to people when sharing access to their smart home devices.

In our pilot survey of 19 people and found that most people were willing to share their smart home devices outside of their home. The most common devices that smart home users wanted to share were smart cameras, home security system for burglar, flood and fire, and smart locks to grant access to the house in case of emergency. Most people preferred to share their smart camera, security system and locks with family members and friends to allow them to access their home for emergencies when they are not home and to monitor and take care of their home and pets.

Through this research, we aim to make the following unique contributions:

* Develop a better understanding of various aspects of sharing of smart home devices from an end-user’s perspective.
* Highlight factors that influence a person’s preferences regarding sharing of smart home devices.
* Provide design-specific recommendation to facilitate further research and development of technology enabling productive sharing of smart home devices among with people outside the home.

# background

In this section we discuss the relevant literature and technologies involved. We first discuss the smart home technology and its intersection with Internet of Things. We then look into trends in smart home privacy and security as it relates to sharing of smart home devices. Finally, look into smart home sharing beyond the home.

**Smart Home Technology and the Internet-of-Things**

The idea of Smart Home has been around since several decades now. The first “wired homes” were built by hobbyists in the early 1960 and the term “smart home” was officially coined in 1984 by the American Association of House Builders [11]. These smart homes largely consisted of stand-alone interactive technologies. Introduction of Internet and advancements in computer networking enabled *things* to communicate over the Internet. Smart Homes Devices could now connect to the Internet which gave birth to Smart Home Internet-of-Things. However not all smart home devices are IoT devices because smart home devices are not necessarily connected to the internet. For example, standalone motion sensor-based lights are a smart home device which are not computer networked. Since only Smart Home IoT devices have the capability to be accessed and shared over the internet, we only focus on these devices and leave out the non-internet-connected smart home devices.

The smart home envisioned by the pioneers never materialized to the general population. Majority of the homes are not smart homes even today. Historically, the key problems associated with slow adoption of smart home have been 1) retrofitting – adding new technology without making major alteration to the existing home; 2) Usability – difficult to use; 3) Lack of Killer Features – Low utility to end users, majority of which believe in “If it ain’t broke, don’t fix it”; 4) Cost; and 5) Interoperability – lack of universal compatibility among smart home devices [12]. The latest advancements in computing, networking and manufacturing has mitigated most of these problems. Reliable wireless technologies like Wi-Fi, Zigbee and Z-wave as well as technologies like Powerline and MoCa facilitating use of existing wires in homes to transmit digital data have eased the retrofitting problem to a great extent. Recent developments in various facets of machine learning and natural language processing have made possible the creation of smart home device (like Personal Voice Assistants) with increased utility. Efforts like Zigbee Alliance [33] and IFTTT [34] are steps towards increased interoperability. Over the years, the cost of smart devices has decreased whereas usability, utility and interoperability have increased. Internet penetration into homes is also at an all-time high today. In 2016, 81 percent of US households had a broadband Internet subscription [5]. Thus, the penetration of smart home technology is at unprecedented levels and finally the smart home is becoming a reality for the masses. It is evident that the major disruptive technology that lead to widespread adoption and success of smart home is Internet of Things and that it is what will drive the future of Smart Home. Existing research on smart homes has focused on the technological challenges involved in delivering smart home environments [8]. Published research on smart homes and their users is growing exponentially, yet a clear understanding of who these users are and how they might use smart home technologies is missing from a field being overwhelmingly pushed by technology developers. Most of the research on smart home technologies has given no consideration to smart home users at all [22].

**Smart Home Privacy and Security**

As the popularity and adoption of Smart Home Internet-of-Things increases so does concerns about privacy and security surrounding the Smart Home Internet-of-Things ecosystem. Research on Smart Home Technology has recognized the challenge of gaining the users’ trust and confidence [10]. Much research has been done related to home IoT has focused on the technical aspects smart home security [1,4,7] whereas few have studied the human aspect of Smart Home Internet-of-Things privacy and security. Zheng et. al studied user perceptions of smart home IoT privacy and reported that users are often willing to sacrifice their privacy for convenience and connectedness [24]. They also found that user opinions about external entities collecting smart home data depend on perceived benefit from these entities. Research on IoT privacy often focus on data leakages, access control, and at the individual level of people inside the home. Kraemer et el. identified that smart home privacy research should be holistic and contextual [14] and argued for a thorough understanding of a home’s socio-cultural context [15]. Chakravorty et al. propose privacy preserving data analytics for smart homes [6]. Research also sheds light on threats and challenges [35], user privacy[16] and primary norms [2] for smart home Internet-of-Things. An emergent theme across this body of work is that the research tends to focus on access control, privacy, and security at the level of an individual or shared among individuals residing within the same home. Less work has examined use cases where smart home devices were shared or could be shared beyond the home. In our study we explore further to understand more about user’s perception of these benefits and external entities. We try to find the exact purpose of sharing of a smart home IoT devices owned by a participant with people outside of their home who they know.

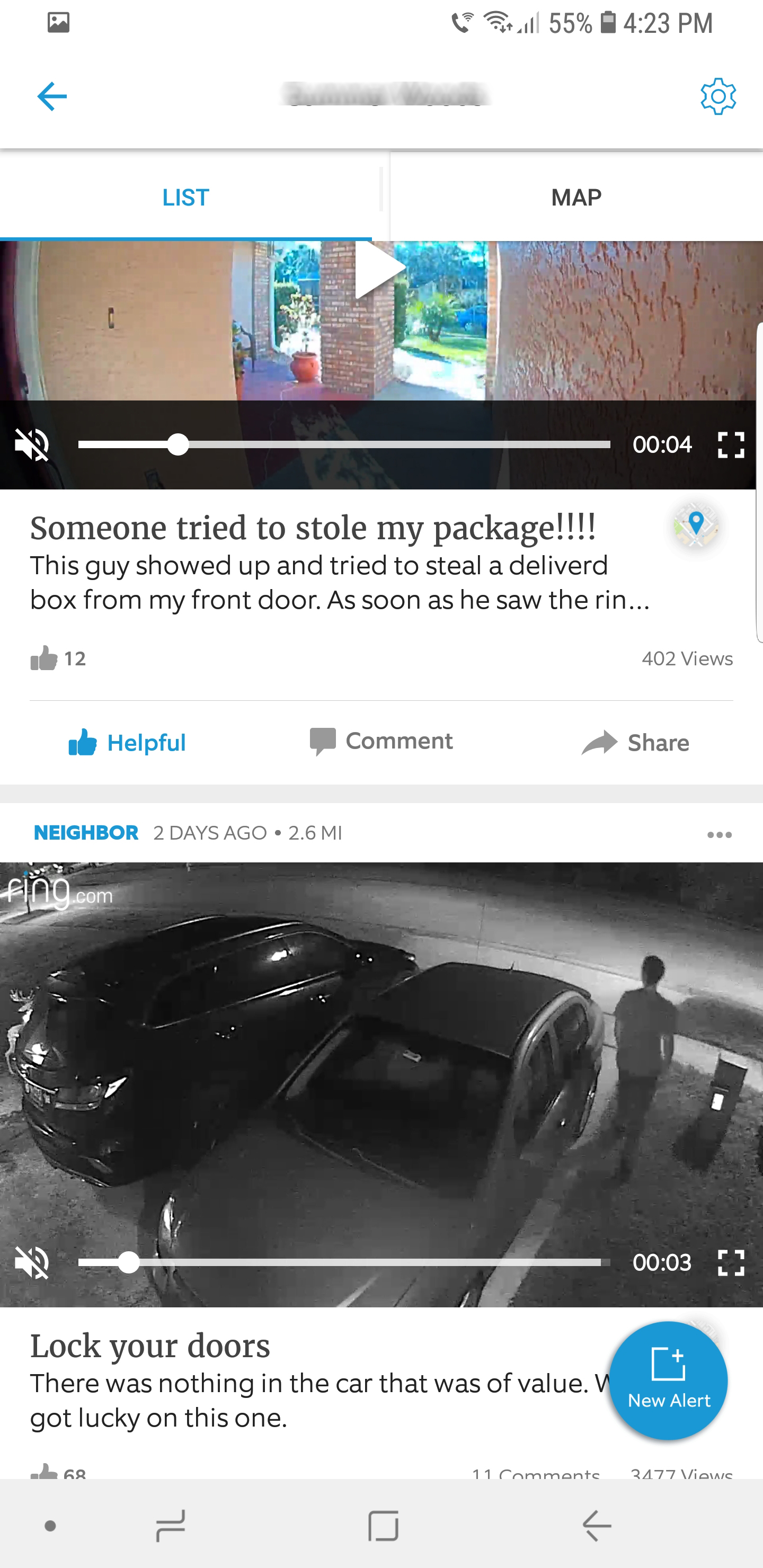
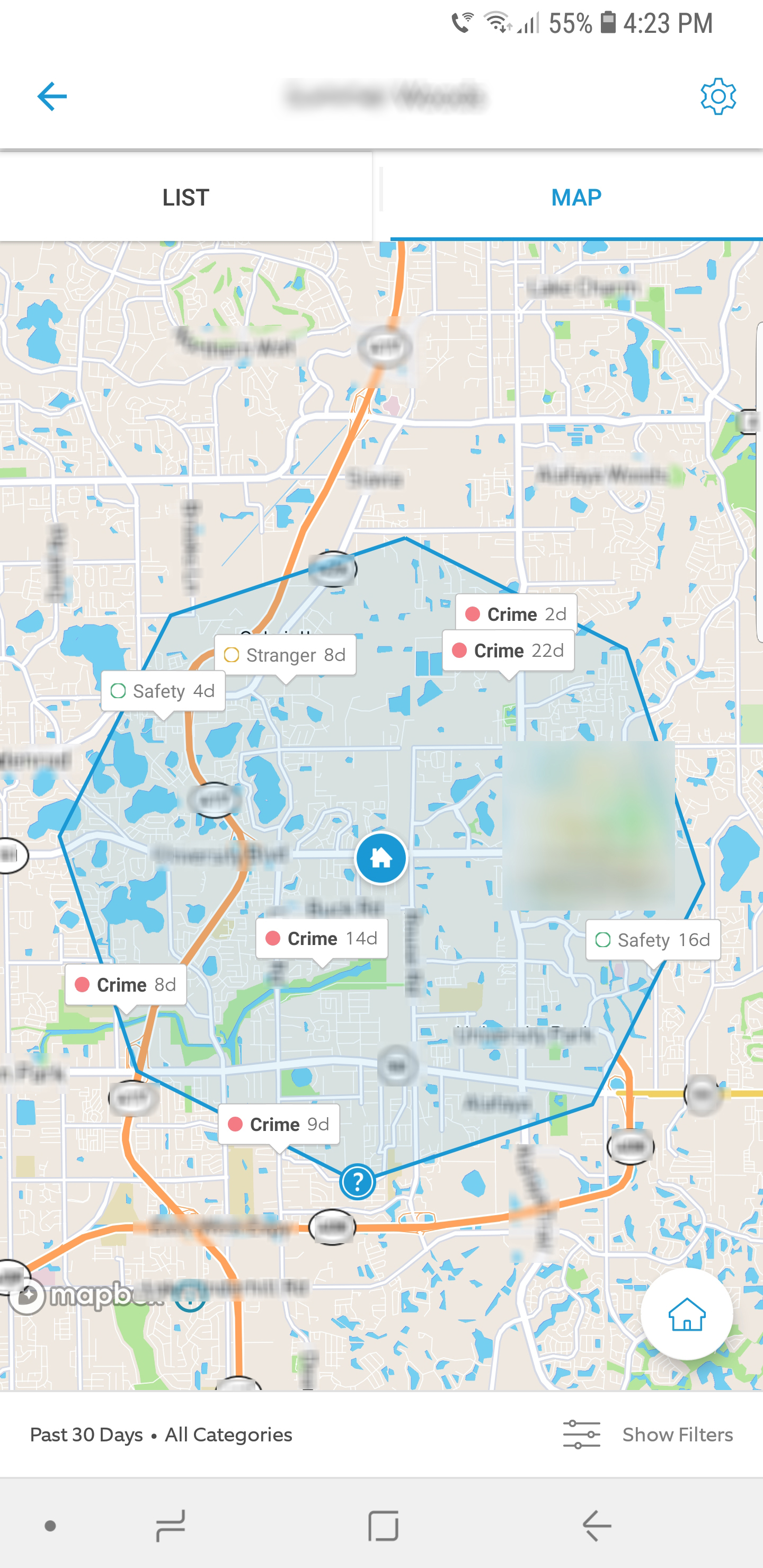
 

Figure : Ring Neighborhood App

**Smart Home Sharing Beyond the Home**

In essence, a smart home collects and analyses data on the domestic environment, relays information to users (and service providers), and enhances the potential for managing different domestic systems (e.g., heating, lighting, entertainment) [9]. Most smart home IoT devices offer some form of access control among users. Often users have the option to share the device with anyone over the Internet. For example, a user can share their Ring doorbell [36] with any person they wish to be able to view who is at their door and get notified with motion is detected by the doorbell and/or when the doorbell rings. This person can be located anywhere in the world as long as they are connected to the internet. Most popular smart home IoT devices and services like Nest learning thermostat [18], Apple Homekit [37] and Wyze Cam [38] all offer similar sharing mechanisms.

Ring Neighborhood App (Figure 1) is another example of sharing data from smart home devices, in particular smart doorbells and cameras. It employs a neighborhood watch system aimed to bring communities together to help create safer neighborhoods. It provides real-time crime and safety alerts from your neighbors, law enforcement and the Ring team [32]. It allows people, at their discretion, to anonymously share videos captured on their camera(s) with their neighbors Fig 4. This presents an interesting case of sharing wherein the data from smart devices is voluntarily and anonymously being shared with known and unknown people in the neighborhood. We incorporated this idea of sharing data from the device rather that then device themselves into the design of our survey.

A survey study by He et al. found that participants' desired access-control policies differed significantly for different capabilities within a single device and the relationship with the person who is trying to use that capability [39]. Their findings suggest that policies about capabilities, rather than devices, better capture users’ preferences. Their work showed the importance of focusing on device capabilities over the devices themselves when examining users’ access control preferences. It also showed that relationship among the people sharing the devices and their location carried significant weighted in home IoT device sharing decisions. We draw findings from this work to influence our survey design. We asked the participants to explain the purpose of sharing each device with each person when asking them to think about the features to be shared and benefit from sharing. We also ask if they would like to share access to the devices of the data originating from those devices. He et al.’s recruited survey participants on Amazon Mechanical Turk [40] and presented them with hypothetical scenarios involving Home IoT access control. While this provided meaningful and valuable data, the participants did not necessarily own or have any experience with the devices in question. To make novel contribution to the body of knowledge, we explore user’s perception surrounding sharing of their actual smart home devices they own and use with people they know. Surveying people who actually own and use smart home devices helps us get better quality data. We intend to better understand the relationships between people sharing the devices as well as specific reasons for sharing of a particular device with a particular person.

# Methods

In this section, we describe our study overview. Then, we discuss survey design, recruitment of participants, participant profile and data analysis approach.

**Study Overview**

We conducted a formative evaluation [3] of users’ needs to understand their potential patterns of sharing of data generated by their smart home devices and access to devices themselves. The user study consisted of an online browser-based survey where each participant was a smart home device user. A survey was suitable for our needs for this study because it made it possible to reach smart home users in a wide geographic location [19]. This makes the data more generalizable. Since we are targeting actual smart home device users, a survey provides an effective medium to reach them as it is easier to accommodate into their busy schedules. It The study was approved by Institutional Review Board.

Initially we required the participants to have everyday access to at least two smart home devices at their primary place of residence (participants 1 to 12). We exclude users with just one smart home device to get better quality data from users who have comparatively more first-hand experience in the smart home ecosystem. In the second iteration of the pilot study (participants 13 to 19), we changed the requirement to just one device to get more data and include the people who owned just one device in our results, making it more generalizable. We used web-based survey platform called Qualtrics [41] to conduct the surveys. The survey questions were designed to explore the sharing preferences of real smart home device users with focus on devices, device features and people involved. We tried to understand the reasons and personal relationships between people who share or are interested in sharing their home IoT devices with each other. We also tried to understand the effect of physical distance between the place of residence between the parties sharing the devices.

**Survey Design**

|  |
| --- |
| Screening Questions  Questions to ideinfity if the participant meants out eligibility criteria |
| Explanation of Research  Participants presented by Explainaiton of Research statement as per IRB protocol for exempt research. |
| Quality Check Question  We asked if the user if they will provide their best answers. Those who indicated that they won’t provide their best answers and those who couldn’t promise either way failed our quality check and their data was discarded. |
| Select Smart Home Devices Owned  This step involved selecting from a list of common devices the smart home devices owned by the participants. Text entries allowed entry of any devices owned which were not listed. |
| List Up to Three People Other Than Those Who Live With you with Whom You Share or Would share Your Smart Home Devices |
| If Not Interested in Sharing with Anyone, Ask why.  Skip to Demographics |
| About people – Relationship and Distance  Participants select the nature of their relationship for each person they listed. They then select where each person lives relative to their home. |
| For each person listed:  Devices to share from the ones owned  Type of sharing – Remote Control, Data, Both  Purpose of sharing each device with each person  Free text entry  Reverse Sharing with this Person? Yes/No  Select devices to Reverse Sharing  Type of sharing – Remote Control, Data Access, Both  Purpose of reverse sharing for each device  Free text entry |
| Demographic Questions  Set of standard demographics questions encompassing things like gender identification, race, employment, education, marital status and household income. |
| Information Regarding Compensation  Code provided to those recruited from mTurk to be redeemed for payment. mTurk ID is collected. |
| Thank you and Optional Feedback on Survey  Participants were presented with a text-box to provide feedback. |

The survey started with a list of smart home IoT devices and the user was asked to select the devices they own. The user also had the option to enter additional devices not included in the list. Only users who select one or more devices proceed with the survey. The users are then asked to list up to three persons with whom they might share their home IoT devices. Information about the participant’s relationship with the persons listed and the proximity of their residence was collected. The participants are then asked which of their smart home IoT devices would they share with the persons they listed. A free-text entry allowed the participants to describe the purpose of sharing the particular device with a particular person. Similar information was collected regarding which smart home IoT devices that the persons listed own which the participant would like to have access to and why. In both cases, the survey asked if the sharing is for devices access, data from the device, or both. Participants then answered questions regarding possible concerns that they might have regarding sharing of smart home IoT devices and how they feel about sharing of these devices in either direction. The survey ended with demographic questions which was intended to allow us to analyze any possible patterns in participants based on their demographic information. The organization of survey questions is presented in table 1.

Table 1: Survey Flow

## Participants Recruitment

For the purpose of running out pilot study we recruited participants using Amazon Mechanical Turk (12) and Word of Mouth (7). The participants were adults residing in the United States. We limited the study to adults in the United States to eliminate differences in perceptions related to differences in societal norms in different countries and also because the United States is by far the biggest market of Smart Home Technology [27]. The survey was designed to take no more than 30 minutes to complete. Twelve participants who were recruited from Amazon Mechanical Turk were paid $1 after their data was verified to be complete and passed our quality check. Those recruited by word of mouth were not compensated.

**Participant Profile**

Age of respondents varied from 23 to 48 years, the mean age being 34.79 years. 82% of the respondents were male whereas 18% were female. Forty five percent of respondents had a bachelor’s degree, 27% had a master’s degree, 18% attended some college but no degree and 9% had an associate degree in college. The annual household income of the respondents varied between $30,000 and 149,999, with two respondents between $60,000 to $69,999, two between $140,000 and $149,000 and one each between $30,000-$39,999, $40,000-$49,999, $50,000-$59,999, $70,000-$79,999, $90,000-$99,999 and $100,000-$119,999. One participant preferred to not disclose his income. Thus, the participants belonged to a fairly diverse income group. 7 participants were married, 3 never married and 1 separated. 5 participants were paid employees, 4 were self-employed and 2 were not working due to disability. Most of the participants (5) worked in management. Other participants worked in computer and mathematical, architecture and engineering, arts design entertainment sports and media, healthcare support, sales and related, and office and support staff.

Figure 2: Most Common Smart Home Devices Owned by Participants

**Data Analysis Approach**

We conducted both quantitative and qualitative analysis of our data to empirically gain insights into a user’s perception and preferences related to sharing of smart home devices with people outside of their home. We generated several new descriptive statistics like which devices smart home IoT users commonly own and wish to share and relationship of people involved. We utilized statistical models to draw several insights like how sharing norms and preferences relate to specific devices and relations between people sharing these devices. We determined the validity of several constructs pertaining to smart home sharing. The qualitative analysis involved testing user’s motivations and purpose of sharing as well as associated concerns relating to privacy and security. Factors contributing to reluctance in sharing were coded and relationship between these factors and other metrics were analyzed to gain insights. Based on these insights, we attempted to propose solutions to inhibition to sharing. Since several of participant’s responses consisted of free-text responses, the qualitative data was iteratively coded. We utilized inductive coding approach for qualitative analysis. A code book capturing the main themes was developed and iteratively improved. This information along with the trends we identified from the users’ responses was used for framing our actionable design-specific recommendation for designing sharing-friendly smart home system.

**Results**

In this section, we present our findings from our pilot survey study of 19 participants.

**Smart Home Devices Owned and Willingness to Share**

The respondents owned an average of 7.07 devices with a standard deviation of 5.4. The most common smart home device was smart TV (15), followed by video streaming device (12), smart speakers or personal voice assistants (12), smart camera (12), motion/contact sensor (10), smart display (10), smart lights (9) and smart thermostat (7). The most common Smart Home devices owned the participants is shown in Figure 2. It was interesting to note that people with more smart home devices usually had higher household incomes that those with fewer devices. This suggests that smart home adoption is more in higher income households, likely due to the cost of the devices.

Out of the 19 people surveyed 14 people were willing to share their smart home devices with people outside of their home whereas 5 people were unwilling. Participants provided various reasons for sharing each device as well as for not sharing anything. Trends in the reasoning provided for both cases are discussed in the following sub-sections on reasons of sharing and reasons for not sharing.

**Devices People Wanted to Share Outside of Their Home**

Most common devices shared with people outside of home (Figure 3) were Smart Camera (6 shares), Security Alarm (4 shares), Motion Sensor (4 shares), Flood Alarm (3 shares) and Smart Lock (3 shares). The primary reason for sharing was safety and security. The most common theme was that security related smart home devices were most likely to be shared with people outside of the home. Other commonly shared devices were entertainment devices where the theme in sharing was saving money on subscriptions. However, this type of sharing was more like sharing of online accounts rather than sharing of smart home devices. We discuss the reasons in detail later in this section.

.

Figure 3: Most Common Smart Home Devices Shared with People Outside of Home

Figure 4: Relationship of respondent with people with whom they would share their smart home devices

Figure 5: Place of primary residence of people with whom respondents would share their smart home devices

**People with Whom Participants Were Willing to Share Their Smart Home Devices**

The survey asked the participants to list up to five people who live outside of their home with whom they would like to share their smart home devices. 33.3% of respondents indicated that they would share their smart home devices with at least one person. Most people who were willing to share their smart home devices outside of their home wanted to do so with their family (40%) and friends (21%). Others wanted to share with a partner or spouse who lived outside the home (15%), co-worker (12%), and acquaintance (12%). The relationship of respondent with people with whom they would share their smart home devices is shown in Figure 5.

The most common place of residence of the people with whom the respondents wanted to share their smart home devices was their home, however this data was discarded as we were only interested in sharing outside of home. The “in my house” option served its purpose by allowing us to filter poor quality data by acting as an attention quality check. It also indicates that most common sharing of smart home devices is within the home. Outside the home, the most common place of residence of the people with whom the respondents wanted to share their smart home devices was “in their country but outside of their state”, followed by “in their town but not in their neighborhood”. Figure 5 shows the Place of primary residence of people with whom respondents would share their smart home devices.

**Reasons for Sharing Smart Home Devices with People Outside of Home**

The participants provided various reasons for sharing their smart home devices with people outside of their home. The most common theme was allowing access to the home for emergency situations and monitoring the home when they are not home. One reason was taking care of the pets when their owners are not home. This often involved sharing of smart locks. Many people wanted to share their smart home IoT devices for security reasons in case of an emergency:

*P1: “Access to the house and know if someone breaks in.”*

When giving their rationale for sharing, a number of participants made references to their pets:

*P2: “If our house was on fire, I would hope someone would try to save our dog.”*

Some people said that they would just share their data for entertainment purposes. One person wanted to share subscriptions to online streaming services to save money.

*P3: “If I don't have cable, I can watch TV without having to pay a bill or we can split the bill. I can share with her music through the smart speaker.”*

The sharing of smart cameras was always data sharing rather than remote control. People wanted to share access to their cameras to trusted family and friends so that they can watch over their homes when they can’t themselves. One person provided the following reason for sharing her camera with a family member who lived out of her state.

*P4: “So that she can access my camera time to time and ensure my house is safe even when I am there or not.”*

She justified sharing her smart doorbell with her family member who lived out of state as follows:

*P4: “For the safety purposes. She can inform me if someone is at my door when I am out for a vacation. I can then act accordingly.”*

In terms of reciprocal sharing, most people preferred to share their smart camera, security system and locks with family members and friends to allow them to access their home for emergencies when they are not home and to monitor and take care of their home and pets.

*P4: “I can inform her if someone breaks in her house and can act accordingly.”*

**Reason for Not Sharing Smart Home Devices with People Outside of Home**

Five people indicated they would not share their smart home devices with anyone outside of their home. Two persons who owned more than 15 smart home devices did not want to share his devices with anyone outside of their home felt no need to share the devices. One of them stated:

*P5: “Currently I do not have anyone needing remote access other than immediate family at the moment and people that watch my house do not need remote access at the moment, they can access via codes on the devices on site. Also, we do not leave the home often enough to worry too much.”*

Another person said he would only share devices with people who don’t live in his house when they are visiting:

*P6: “The only time I would likely share access to my smart home devices with people who do not live in my house will be when they are visiting for a prolonged period of time. For example, if I have a guest staying over, I will provide access to their lights, fan and smart speaker in the guest bedroom. Of course, anybody staying over will physically have access to almost all of my smart home devices like lights, thermostat, smart TV and robot vacuum. They can issue voice commands to control most devices when they are in home, but that does not mean they will be getting their own account or login.”*

Other participants were primarily concerned about privacy and security breaches, even from the device manufacturers themselves:

*P7: “I don’t want anyone spying on me; I especially don’t want Amazon or the government spying on me!”*

# Discussion

In this section, we discuss design implications that evolved from the study. At the end, we provide limitations of our work and point out future direction of this research.

**Relationships Matter More Than Distance**

People wanted to share their smart home devices with the people they trust, like their family and friends, regardless of the physical distance between them. Same was true for reciprocal sharing. This suggests that smart home users are more likely to share their devices with a family member or friend living out of state than their next-door neighbor. Thus, trust is an important factor affecting smart home users’ decision on sharing of their devices outside of their home.

**Recommendations for Design**

We discuss the design implications from our user study in the sub-sections below.

### Smart Home Security Devices Must Incorporate Remote Sharing Feature

We found that most people are willing to share their smart home devices like smart cameras and home security systems outside of their home to grant access to the house to their friends and family in case of an emergency and to watch over their property when they are not home. Smart Home security systems must allow for such sharing. Additionally, it goes without saying that such sharing should be secured to the maximum extent employing best encryption and authentication protocols due to the highly critical nature of these devices.

### Conditional Sharing Based on Presence in Home

A common theme in sharing involved action that the person with whom the devices the shared would perform when the device owner is not available. As such it would be useful to have systems that would allow conditional sharing based on factors like the presence of device owner in the home. Sharing security devices only when intended (like only when the device owner is not home), it would not only reduce the load on the person with whom the device is share but also increase the privacy of the device owner. For instance, consider a smart camera or doorbell only sends notifications to a person outside of home when the device owner is not home or unavailable. This would ensure that the person with whom the device is shared only receives useful notifications and that the privacy of the person sharing the device is protected when he/she is home and available.

### The Utility in Sharing Should be Made Visible

Two of the five people who indicated that they would not like to share anyone outside of their home said they saw no reason to do so. While this is a valid argument for nonuse, it is also possible that they are not aware of some utility of sharing their devices outside of their home. Smart Home system designers who incorporate remote sharing features should make sure that the utility of sharing is either obvious or clearly presented to the user. If the sharing provides non-intuitive new benefits or involves atypical use-cases, the user should be made aware so that they can make better informed decisions.

### Security Should Be Central to Smart Home (Sharing) Design

Two of the five people who did not want to share their smart home devices with anyone outside of their home expressed concerns over privacy and security not only in sharing but in the overall use of smart home devices. Remarkably, we found that security was also one of the key motivations for sharing smart home devices with people outside of home. This suggests that users are likely to use and share smart home devices if they feel confident that it is secure. Users who are employing smart home devices to security application are willing to share these devices with people outside of their home for increased security that comes with having a remote person monitor the security devices.

*Temporary Sharing Feature for Visitors*

People also wanted to share the devices with their visitors. This suggests that smart home systems should have features for quick and easy sharing for visitors. This sharing should also be temporary in nature and can be limited based on time or location.

**Limitations and Future Work**

Although our survey was limited to U.S. residents, it still gave us good insights into people’s perspective on smart home sharing outside of home since U.S. has the highest smart home penetration in the world [27] and thus represents ideal population to study who represent the bulk of smart home users in the world. We only surveyed a small sample of participants, 19 individuals. Our study also suffered from the problems inherent to any self-reported data. The participants may not be completely honest and what they say in a survey may differ from what they do in reality. Also, since we recruited participants form Amazon Mechanical Turk, the data we received from was not very high quality and did not provide as much meaningful insights as we would have liked.

In the future, we would like to conduct the survey with 200 participants to gain more insights. For this survey, we will not recruit participants on Amazon Mechanical Turk but look for other recruiting solutions like Qualtrics panel services. Future studies can also include participants outside of the United States to analyze a wider spectrum of smart home sharing perspectives across the globe. Additionally, future work may possibly incorporate the APIs from various smart home device providers to collect actual data on the smart home devices and their sharing settings. This would help overcome some of the limitations associated with self-reported data. Such data combined with self-reported data collected by means of survey can possibly facilitate in new insights into this field of smart home sharing beyond and within the home.

# CONCLUSION

We explored the end user’s perception of smart home sharing. We found that most people are willing to share their smart home devices like smart cameras and home security systems outside of their home to grant access to the house to their friends and family in case of an emergency and to watch over their property when they are not home. Trust is the important factor affecting smart home users’ decision on sharing of their devices outside of their home. People wanted to share with the people they trust like their family and friends regardless of the physical distance between them. Those choosing not to share their smart home devices with anybody outside of their home either say no use of such sharing or were concerned about the security and privacy. People also want to temporarily share their smart home devices with their guests who they visit their home.

**ACKNOWLEDGMENT**

This research was supported by the Mozilla Research under grant xxxxxx (anonymized for review). 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 Mozilla Research Foundation.

# REFERENCES

1. Noah Apthorpe, Dillon Reisman, and Nick Feamster. 2017. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. Retrieved October 19, 2018 from https://arxiv.org/abs/1705.06805

2. Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2: 59:1–59:23. https://doi.org/10.1145/3214262

3. Benjamin S. Bloom and And Others. 1971. *Handbook on Formative and Summative Evaluation of Student Learning*. McGraw-Hill Book Company, 330 West 42nd Street, New York, New York 10036 ($11.

4. J. Bugeja, A. Jacobsson, and P. Davidsson. 2016. On Privacy and Security Challenges in Smart Connected Homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*, 172–175. https://doi.org/10.1109/EISIC.2016.044

5. US Census Bureau. Computer and Internet Use in the United States: 2016. Retrieved September 25, 2018 from https://www.census.gov/library/publications/2018/acs/acs-39.html

6. Antorweep Chakravorty, Tomasz Wlodarczyk, and Chunming Rong. 2013. Privacy Preserving Data Analytics for Smart Homes. 23–27. https://doi.org/10.1109/SPW.2013.22

7. Mauro Conti, Michele Nati, Enrico Rotundo, and Riccardo Spolaor. 2016. Mind The Plug! Laptop-User Recognition Through Power Consumption. In *Proceedings of the 2Nd ACM International Workshop on IoT Privacy, Trust, and Security* (IoTPTS ’16), 37–44. https://doi.org/10.1145/2899007.2899009

8. Diane J. Cook. 2012. How Smart Is Your Home? *Science* 335, 6076: 1579–1581. https://doi.org/10.1126/science.1217640

9. Steven K. Firth, Farid Fouchal, Tom Kane, Vanda Dimitriou, and Tarek M. Hassan. 2013. Decision support systems for domestic retrofit provision using smart home data streams. *CIB W78 2013 30th International Conference on Applications of IT in the AEC Industry*. Retrieved December 6, 2018 from https://dspace.lboro.ac.uk/dspace-jspui/handle/2134/15904

10. E. Harms. 2015. Smart home—good things come to those who wait. In *8th international conference on energy efficiency in domestic appliances and lighting (EEDAL’15), Luzern, Switzerland*, 26–18.

11. Richard Harper. 2003. Inside the Smart Home: Ideas, Possibilities and Methods. In *Inside the Smart Home*, Richard Harper (ed.). Springer London, London, 1–13. https://doi.org/10.1007/1-85233-854-7\_1

12. Patrick Holroyd, Phil Watten, and Paul Newbury. 2010. Why Is My Home Not Smart? In *Aging Friendly Technology for Health and Independence* (Lecture Notes in Computer Science), 53–59.

13. Hermann Kopetz. 2011. Internet of Things. In *Real-Time Systems: Design Principles for Distributed Embedded Applications*, Hermann Kopetz (ed.). Springer US, Boston, MA, 307–323. https://doi.org/10.1007/978-1-4419-8237-7\_13

14. M. J. Kraemer and I. Flechais. 2018. Researching Privacy in Smart Homes: A Roadmap of Future Directions and Research Methods. 38 (10 pp.)-38 (10 pp.). https://doi.org/10.1049/cp.2018.0038

15. Martin J. Kraemer. 2018. Preserving Privacy in Smart Homes: A Socio-Cultural Approach. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI EA ’18), DC12:1–DC12:4. https://doi.org/10.1145/3170427.3173018

16. H. Lee and A. Kobsa. 2016. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 407–412. https://doi.org/10.1109/WF-IoT.2016.7845392

17. Roberto Minerva, Abyi Biru, and Domenico Rotondi. 2015. Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative* 1: 1–86.

18. Nest. Nest Learning Thermostat | Programs Itself Then Pays for Itself. *Nest*. Retrieved October 19, 2018 from https://www.nest.com/thermostats/nest-learning-thermostat/overview/

19. A. Ant Ozok. 2009. Survey design and implementation in HCI. *Human-Computer Interaction: Development Process* 253.

20. J Sukanya, A Ramya, and S Vijayakumar. SMART MOBILE APP DEVELOPMENT: SECURITY ISSUES AND CHALLENGES. 6.

21. Liam Tung. ​IoT devices will outnumber the world’s population this year for the first time. *ZDNet*. Retrieved December 7, 2018 from https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

22. Charlie Wilson, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2015. Smart homes and their users: a systematic analysis and key challenges. *Personal and Ubiquitous Computing* 19, 2: 463–476. https://doi.org/10.1007/s00779-014-0813-0

23. Feng Xia, Laurence T. Yang, Lizhe Wang, and Alexey Vinel. 2012. Internet of Things. *International Journal of Communication Systems* 25, 9: 1101–1102. https://doi.org/10.1002/dac.2417

24. Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *arXiv:1802.08182 [cs]*. https://doi.org/10.1145/3274469

25. 2015. Amazon Echo is now available for everyone to buy for $179.99, shipments start on July 14. *Android Central*. Retrieved September 25, 2018 from https://www.androidcentral.com/amazon-echo-now-available-everyone-buy-17999-shipments-start-july-14

26. There are officially more mobile devices than people in the world | The Independent. Retrieved December 7, 2018 from https://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

27. Smart Home - United States | Statista Market Forecast. *Statista*. Retrieved September 24, 2018 from https://www.statista.com/outlook/279/109/smart-home/united-states

28. Smart Speaker Penetration Hits 20% of U.S. Wi-Fi Households. *comScore, Inc.* Retrieved September 24, 2018 from http://www.comscore.com/Insights/Blog/Smart-Speaker-Penetration-Hits-20-Percent-of-US-Wi-Fi-Households

29. Google Home to sell for $129, launches on November 4. *CNET*. Retrieved September 25, 2018 from https://www.cnet.com/news/google-home-to-sell-for-129-launches-on-november-4/

30. Google Home will go on sale today for $129, shipping November 4. *TechCrunch*. Retrieved September 25, 2018 from http://social.techcrunch.com/2016/10/04/say-hello-to-google-home/

31. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper. *Cisco*. Retrieved September 24, 2018 from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

32. Get Real-Time Crime and Safety Alerts With the Neighbors App | Ring. Retrieved November 22, 2018 from https://ring.com/neighbors

33. Zigbee Alliance. *Zigbee Alliance*. Retrieved October 19, 2018 from https://www.zigbee.org/

34. IFTTT helps your apps and devices work together. Retrieved October 19, 2018 from https://ifttt.com/

35. Privacy in the Internet of Things: Threats and Challenges | Request PDF. *ResearchGate*. http://dx.doi.org/10.1002/sec.795

36. Video Doorbells. *Ring Team*. Retrieved October 19, 2018 from https://shop.ring.com/collections/video-doorbells

37. iOS - Home. *Apple*. Retrieved October 19, 2018 from https://www.apple.com/ios/home/

38. Home. *WyzeCam*. Retrieved October 19, 2018 from https://www.wyzecam.com/

39. Rethinking Access Control and Authentication for the Home Internet of Things (IoT) | USENIX. Retrieved October 18, 2018 from https://www.usenix.org/conference/usenixsecurity18/presentation/he

40. Amazon Mechanical Turk. Retrieved October 19, 2018 from https://www.mturk.com/

41. The Leading Research & Experience Software. *Qualtrics*. Retrieved September 25, 2018 from https://www.qualtrics.com/