University of Cincinnati

Date: 3/15/2022

I, Prateek Muneesh Chellani, hereby submit this original work as part of the requirements for the degree of Master of Science in Information Technology.

It is entitled:

Remote Device Sharing in Smart-Homes: Explained by Cultural Differences

Student's name: **Prateek Muneesh Chellani**

This work and its defense approved by:

Committee chair: Jess Kropczynski, Ph.D.

Committee member: Nora McDonald, Ph.D.

41832

Remote Device Sharing in Smart-Homes: Explained by Cultural Differences

A thesis submitted to the

Graduate School

of the University of Cincinnati

in partial fulfillment of the

requirements for the degree of

Master of Science

in the School of Information Technology

of the College of Education, Criminal Justice, and Human Services

by

Prateek M. Chellani

2022

Committee Chair: Dr. Jessica Kropczynski, AD Graduate Education and Graduate Director

,

Abstract

With families increasingly moving towards smart devices and home automation, the right security policies and access control are essential. However, in multi-person and family homes, several users are sharing an IoT device, bringing up the question of who's in control. We examine how smart-home owners share their IoT devices, and how they feel about using sharing features. In a global landscape, understanding cultural differences is key in every field, and IoT is no different. Using a mixture of survey and interview methods, we collect data regarding smart-home owners' IoT devices, specifically which of these devices they share, their preferences for sharing, and why. We then explore the role that cultural differences have on device sharing.

Dedication

I am extremely grateful to several people for motivating and assisting me in conducting this thesis.

While it's near impossible to acknowledge everyone, I'd like to mention my parents and family who encouraged me to take on this topic,

My advisor, Dr. Jess, who guided me through the process,

My committee member Dr. Nora, who provided insightful and timely feedback,

All the survey and interview participants who were extremely cooperative throughout the study,

and my friends, who helped me refine the idea when initially starting out on the study.

Table of Contents

List of Tables

List of Figures

List of Acronyms

IoT: Internet of Things

RQ: Research Questions

SOHO: Small Office/Home Office

APIs: Application Programming Interface

TVs: Televisions

1 Remote Device Sharing in Smart-Homes: Explained by Cultural Differences

1.1 Introduction

With ubiquity of smart devices, users are becoming increasingly capable of accessing their homes remotely. Regardless of whether it is to turn on the heater, stream sports, or check in on a toddler, remote access using smart home devices is slowly becoming an integral part of our lifestyle. However, one aspect of remote access that has not been tapped into yet is remote device sharing. The ability to share access to your home automation or security devices with a neighbor or a close friend in case of emergencies may be indispensable. Yet a study by Tabassum et al. [TKWRL20] found that nearly 50 percent of Smart-Home owners refused to share remote access to any of their IoT devices. On the other hand, not sharing devices presents certain benefits and safeguards in terms of privacy, safety, and surveillance. In fact, given the lack of clear benefits that users may gain from device sharing, it is difficult to evaluate whether the privacy trade-offs are worth it. Most IoT Devices have at least some form of rudimentary access controls that allow for remote sharing. Existing research focuses largely on the average American user and their interaction with these features, as well as whether they choose to share access. However, there's little data that accounts for cultural differences and whether the factors that influence willingness to share devices vary across countries. Research into what would make people more comfortable sharing their IoT devices with people outside their homes could go a long way when it comes to improving smart-home security for a more broader set of users and cultures. The research questions for our study include:

- RQ1: How are people sharing smart home device and how does that relate to cultural experience and background?

- RQ2: How do cultural differences impact perceptions of privacy as it relates to IoT and device sharing?
- RQ3: What features, policies or data flows do individuals of different cultures believe would help or hinder sharing of IoT devices?

1.2 Background Literature

Several studies have attempted to examine the concept of smart homes and the various interactions within. However, there is limited research regarding how cultural variances account for differences in device sharing needs.

1.2.1 Device Sharing and Access Control

The majority of IoT sharing and access control research is focuses on device access control (most often, situational access control) privacy. These privacy studies are focused on the high-level analysis of privacy, functionality, and the tug of war between the two, usually culminating in the fact that privacy and IoT adoption are mutually exclusive.

Agrawal et al. found that “smart home users desire [a] more complex access control system than what is offered” [ABB^{+}20]. Current vendors offer a “binary option to either share permanent access or not” [ABB^{+}20] that force users to share all features of the device, which may not always be desirable. Based on their study, it’s easy to notice a gap in the current offerings and the features desired by users, particularly regarding having more detailed options to share access, such as setting fixed times to share at.

A study by Mazurek found that most people have significant amounts of data they want to protect, and claimed that existing smart devices lack adequate features for doing so. [MAB^{+}20]. When users were asked questions on potential access control systems several common observations were found. Location played a large factor. Users were more likely to grant access in their home than in other environments, and further added “guests in the participants’ homes were presumed to be trusted” [MAB$^+$20]. Users wanted the ability to quickly and easily remove permissions that had been granted previously.

In another research conducted by Schuster, et. al, the authors talk more about the access control problem, and state that “access control in IoT is fundamentally decentralized” [SST18]. Most devices have their own authentication and sharing permissions and often retrieve and provide access to data from various API’s that have their own permissions. Schuster, et. al. further explored platform permissions by means of ‘constraint’ settings, commonly known as ‘scenes’ on many platforms. Examples of desired future state like, “Allow access but notify the user”, “Allow access but log the operation”, “Allow access only when user is not at home”, “Allow access only when user is at work”, “Allow access only when user is awake”, “Allow access only during an emergency”. They found that these desired features were common across a variety of participants, suggesting that there exists a need for such features.

He et al. look into user preferences regarding access control and find what access control policies users’ would like to see and use. Their study, administered through an online survey examines what individuals believe the best suited default policy should be, while extending their study to look into authentication methods [HGP$^+$18].

1.2.2 Smart Homes and Privacy

Zheng conducted interviews with smart-home device owners and found that a primary subject was privacy, “themes indicate that users prioritize convenience and connectedness, and these values dictate their privacy opinions and behaviors”. These findings mirror what many others have found that IoT is a distributed system, “findings provide new evidence of users’ IoT-specific privacy considerations and suggest the need for improved privacy notifications and user-friendly settings, as well as industry privacy standards that cut across regulatory divisions” [ZACF18].

Mantas et al. talks about the primary security objectives that smart-homes and smart-home devices are expected to fulfill, and notes Confidentiality, Integrity, Authentication, Authorization, Non-repudiation and Availability. Confidentiality refers to the privacy of the information stored on devices within the smart home[MLK10]. Authentication builds on this and requires that only authorized people can use the IoT devices as intended. Confidentiality and Authentication both play a critical role when examining device sharing, as it ties into user-roles and only partially sharing certain features of a device. Well designed access control helps smart-home devices fulfill these five criteria outlined by Mantas and as a whole, help reduce the privacy risk associated with device sharing.

Remote sharing requires increased focus on authentication and confidentiality too, as allowing information (such as data from a smart thermostat, for example) to be shared over the internet makes it more vulnerable to being intercepted. However, the probability of a malicious attack isn't solely dependent on remote sharing. Yoon, et. al hypothesized that "as the number of devices in a smart home increases, so does the chance of a malicious attack." [YPY17]

1.2.3 Cultural Variation and Hofstede's Theory in IT

A survey study conducted by Sabri et al. analyzed the impact of culture on IoT technology, and the willingness of universities in Saudi Arabia to adopt IoT technology. The study utilized cultural dimensions from another study, proposed by Geert Hofstede and found that Femininity, Power Distance, Long-Term Orientation and Individualism were the four cultural dimensions that had an effect on the universities' willingness to adopt and implement IoT technologies. They demonstrated that low individualism and low uncertainty avoidance scores were key to the adoption of IoT technology. While this study doesn't discuss device sharing and smart-home IoT devices, they're generalized approach to all IoT technologies can be extended to provide a baseline of expected results for this study. [SHZ20]

Another paper by Cho and Kim used a cross-cultural study between the United States and South Korea to examine the cultural differences between the two countries regarding crowdfunded projects. This study also took into account Hofstede's insights and found that crowdfunded sites in South Korea demonstrated high levels of collectivism, while American sites demonstrated high levels of individualism. [CK17] Their findings were consistent with Hofstede's dimensions regarding the United States and South Korea.

1.3 Methods

We used two complementary data collection methods to understand smart-home users' remote-sharing needs. Initially, we employed a survey that collects information about home automation device owners, their demographics, who they share their devices with within the home and remotely, and what some potential reasons for sharing these devices may be.

We then interviewed smart-device owners to better understand how they share their devices and why. We also used findings from the survey and interview to understand the relationship between sharing practices and cultural backgrounds.

1.3.1 Online survey study

Given the extensive research that exists on the user preferences and privacy perceptions of smart-home devices among the American population [TKWRL20], we'd chose to target an international demographic and perform a comparative study. Similar data was collected for an Indian population, as well as an American population to have a baseline to compare to. The survey audience was aimed at adult smart-home owners that own (or co-own) their homes. We chose not to put an age ceiling on the audience, as we believe it can help us get a diverse picture. The two countries chosen, India and the United states, were chosen as we believe that these countries have to significantly varying cultures. We also had a small overlap of cultures, with people of mixed cultural backgrounds providing key data in understanding how device sharing needs vary by generation and what impact the environment has.

The survey was be hosted on Qualtrics, an online platform, which is provided by the University of Cincinnati. Potential participants were identified through personal networks and smart-home forums and were thanked for their time. In addition to this, four participants were randomly chosen for an Amazon gift card worth $10.

The list of questions used for the survey are in Appendix 1. The survey borrows several questions from the [HGP+18] study, which administered a similar online survey to better understand user preferences regarding access control.

1.3.2 Interview study

We reached out to survey respondents across the sample for a 1-on-1 interview, if they opt-in to choosing to be interviewed. Respondents were chosen from a subset across the survey sample to reduce bias. The interview was conducted virtually, over Microsoft Teams. However, participants that don't have access to Microsoft Teams were also given the option to chose another video conferencing platform of their choice. We then conducted semi-structured interviews focusing on use of current IoT devices, such as their awareness and use of the sharing features and their current sharing practices and perceptions. Next, we chose to focus on understanding the participants' perceptions about their current IoT devices' sharing capabilities, and whether they've had any experience sharing these devices in the past. The interviewee was also encouraged to discuss what they could potentially gain out of sharing their device, and what they may lose by doing so. The interviewee was later asked to reflect on whether there are circumstances they would like to share more but can't. Finally, we spoke about the participants cultural backgrounds and technology familiarity and perceptions of the impact of their experience and background on sharing practices. Each interview lasted about 45 minutes on average, with participants being encouraged to ensure their availability for at least one hour. All interview participants were compensated for their time with an Amazon gift card worth $10. We believe that using these questions to elicit qualitative responses from the interviewees helped us truly understand what a participant is looking for from their Smart Device when it comes to sharing needs. We also expect these results to help understand how culture impacts IoT technology across borders, and whether smart devices of the future should be targeted towards a particular audience. Table 1.1 shows the participants interviewed and their demographics.

1.3.3 Analysis

From the survey, data collected was primarily numerical which we used to create averages for each culture or nationality, in order to compare them. Questions such as ”Why do you share X device with Y person” were asked in the survey and helped educate us as to some of the basic reasons as to why people might share devices. Google Sheets was used for analysis, as they offered integration with Qualtrics.

For the interviews, we chose to use thematic analysis to better interpret interview responses. Thematic Analysis is a method described by Braun and Clarke to identify patterns in qualitative data and interpret them in a meaningful manner. [CB17] Interview responses were used to create user themes and profiles, identifying several different types of users across the two countries. Interviews were conducted until we reach saturation. Interviews were recorded and stored within UC’s OneDrive, a secure platform to house these recordings. Recordings were referred to several times to gain a better understanding of user preferences.

Table 1.1: Sociodemographic Characteristics of Participants

Alias	Age	Sex	Job	No. of Devices	Shares with	Resides	Influences
Adam	43	Male	Medical	2	Spouse	India	N/A
Brian	40	Male	Finance	1	Spouse, Mother	India	N/A
Colin	50	Male	Sales	2	Spouse, In-Laws, Child, House-help	India	N/A
David	50	Male	Marketing	2	Spouse, In-Law, Children	India	N/A
Eric	31	Male	IT	3	Spouse	USA	India
Fiona	20	Female	Unempl.	5	Mother	USA	Jamaica
Georgia	48	Female	Education	6	Spouse, Children, Sibling	USA	N/A
Henry	47	Male	IT	4	No One	USA	N/A

1.4 Results

The first set of results we received was from participants' responses to the survey. We aggregated these results to learn some descriptive statistics about our user base.

1.4.1 Participant Demographics and Characteristics

The survey was completed by 41 participants, with 28 of these being based in the United States and the remainder being either from India or of Indian origin. Of the 28 participants from the United States, two reported that they were of Indian origin or had lived in India in the past. Some participants also reported having ancestry from Jamaica, the Philippines, China and various European nations. Figure 1.1 shows the cultural background of the American or Indian respondents that stated they had direct cultural influences from other cultures. The average age of the respondents was 33 years old. 26% were females, while the other 74% were males. The studied population was well educated, with 30 participants having completed a Bachelor's Degree or higher. The average number of people in a home in addition to a respondent was slightly more than two. The studied population was well balanced in terms of occupation, with Education and Business being the two most popular industries for the respondents. Of the 41 participants, 37 held full-time positions, while two others were students, one was unemployed and one chose to not disclose this information.

1.4.2 The Devices

The most common devices listed were Smart TVs, with 25 people owning and sharing a Smart TV. Of these, 5 were Indians, while the other were Americans. Other popular devices that were listed were Speakers or Personal Voice Assistants (15), Video streaming devices (12) and smart cameras (8). 60% percentage of participants also indicated that they expected reciprocation of sharing on devices. Figure 1.2 below shows a complete breakdown of devices that the subjects owned.

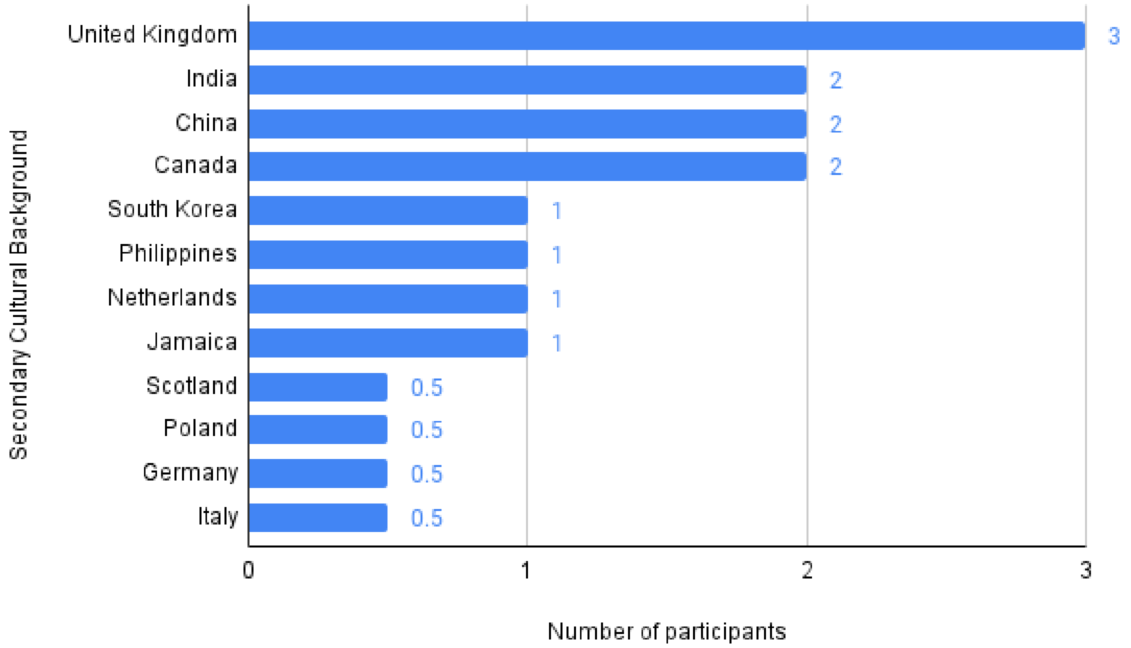

Figure 1.1: Secondary Cultural Backgrounds of participants. Note, 2 people reporting Indian backgrounds were not the only Indians in the study. They were the only two Americans of Indian origin

1.4.3 Current Device Sharing

Participants from both India and the United States most often reported sharing devices with their spouses (42.8%), followed by their friends(21.4%) and visiting family(21.4%).Figure 1 shows the most popular roles that people listed when mentioning who they share their devices with.

When it comes to remote sharing, there was a noticeable difference between users from the US and India. In general, users in the US were more likely to share devices with someone remotely than Indians. The most common people that had access to a device was unsurprising those who lived in the same home, a common response independent of culture. However, the second most was people that lived in a different city and were visiting.

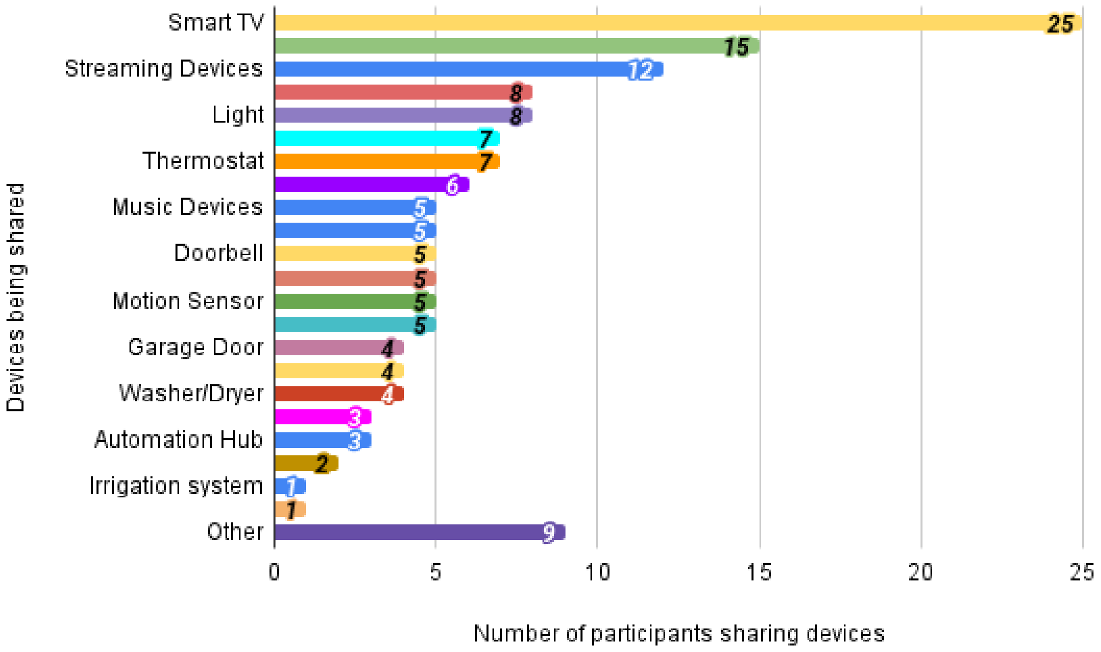

Figure 1.2: Devices owned by survey respondents

1.4.4 The Interview

Based on the interview, there were two particular types of participants that emerged. The first type of participant was the Private type (n=4). This participant was tech-savvy and owned several devices, and was comfortable sharing the devices to varying degrees, often utilizing privacy controls and only sharing as needed. As a result, Private participants only shared devices on a need-to-need basis, best illustrated by this quote, ”Even if the privacy risks are minimal with sharing some devices, they still exist, and I'd prefer to be safe by not sharing if avoidable.” The quote can sum up the group of Private participants fairly well, as they didn't want to share access to a device if the sharing capabilities were unlikely to be used. Another participant from the same group also talked about the sheer volume of data that your giving access to by sharing. ”There is too much of personal data on most of your devices in today's day and age.”

However, at the same time, these participants also were okay sharing if it meant increased convenience. One example was that of the Smart-Door lock, and sharing access with a non-family member who required daily access (such as a babysitter). A participant who was involved in multiple virtual meetings didn’t want to have to open the door to the babysitter daily, and to avoid this, set up ”unrestricted” access for the baby sitter as well. ”It’s a trade-off between convenience and privacy.”

On the other hand, participants of the other type, the Trusting type (n=4), generally were more trusting and willing to share access to anything with those they trusted, without the need for a reason. ”They are family, and I trust them with everything, just as much as they trust me. If someone I trust that much is violating my trust, then device data is the least of my concerns.” While many participants did note that sharing their devices didn’t necessarily equate to sharing private information, they also acknowledged that the people they share devices with, they’d trust with that information anyway. One standout example was when a participant talked about sharing access to their laptop with visiting friends or family. They mentioned that while it is unusual in this day and age to share laptops, there are times when a visitor’s laptop may run into issues or they may need a laptop for some emergency work. ”Ideally when I share a device even with the closest people, it is done in a way that none of my privacy is violated at all.” However, they said this is still a trust-based system, using features such as Chrome profiles to avoid running into each others personal files. They mentioned that in an ideal world, this system wouldn’t be trust-based, and there would be other options to share.

Coming back to the example of smart-door lock though, the second type of participant was more reluctant to share access to anyone but the adults that live within their house. They mentioned that if a One-Time Password system or buzzer system to buzz guests in existed, they’d prefer that, but if not, they would not give any form of access to ’outsiders’, even if it meant opening the door multiple times a day themselves.

1.4.5 Cultural Influences

With two distinct cultures being surveyed, there was some visible variances when it came to the demographics. The population based in India was generally older, with an average age of 42.3, in comparison to an average age of 32.48 in the United States. The number of people in each household on average was also larger, with there being 3.6 people in the house of each respondent from India in addition to the respondent themselves, as opposed to 1.83 in the United States. Lastly, another noticeable difference was with the number of smart-home devices owned. Indian respondents indicated 2.3 devices on average, while Americans had an average of 8.72 (12 American respondents mentioned they had 15+ smart-home devices, the highest category in the survey. For calculation purposes, 16 was used).

One interesting stand-out across cultures in the interview was that participants of the Private type were mostly American, while all the participants of the Trusting type were Indian. This is note-worthy as it shows the variance across cultures when it comes to device sharing. While all eight participants specified that they only shared devices with people they trust and had somewhat similar survey responses, the extent to which they needed to trust someone and the size of their circle of trust varied significantly.

Based on survey responses, of the two participants that reported both Indian and American influences, their responses were closer to the average American response. Only one of the participants that had experienced both cultures took part in the interview, and reported that their culture wasn't the primary decider behind their decisions, attributing their choices to a mixture of culture, upbringing, and personality. They described themselves as " a trusting person but also a creature of habit and roles", suggesting that they like to believe that if they were to share devices with someone, it'd likely be because they trust them and expect them to not violate the trust.

They did also mention that they believe how strongly a culture influences sharing preferences varies significantly from device to device. ””I don’t think culture applies as much to some devices such as a SMART TV, which almost everyone would share unless it’s conflicting with their use.

While their survey responses were closer to the average American response when it came to demographics as well as sharing practices, their interview responses varied from the average American response, as the interviewed participants mentioned that they wouldn’t share any device unless needed, much like the other participants of the Trusting type.

1.4.6 Reasons to Share Device Access

In addition to just understanding cultural influences, this study also attempted to understand the reasons people share (or don’t) any of their devices. Based on both the survey and interview responses, the most popular reason to share seemed to be convenience related - people were comfortable sharing devices they owned with others in their home for mutual benefit.

For example, Colin, who lives in a single family, 5 person home talked about why he unrestricted shares access to his smart TV with everyone in the home, mentioning that the TV was ”co-owned” in a way, and that it was there for the entertainment of the entire family. ”If I’m not using it [TV], it doesn’t make sense to prevent someone from using it to entertain themselves. Even if I was planning on using it, I’d let them use it too, as it’s just easier than everyone having to get a TV of their own.” David, another participant, echoed the same thoughts, also mentioning ”compromise is a part of living with someone” and stated that they’ve never run into conflicts about sharing smart devices, and the unspoken rule in their home is that ”everyone in the house can use every device.”

Another common reason to share smart devices within the home was a financial one. Even though the surveyed audience had a higher than average household income and were generally doing well, many agreed that it didn't seem fiscally prudent to purchase multiple identical devices.

In the survey, another popular response was from parents sharing access to their cameras or baby monitors with their spouses. The reasons for this were fairly obvious, as the respondents were all married couples that shared joint custody of their child and were both equally responsible and interested in the child's well-being. Responses varied from a simple ”for watching our kids” to more detailed responses on why both parents needed unrestricted access to the camera at all times. Two respondents also included their baby-sitter under the same reason, sharing access to a baby monitor, while some others also mentioned sharing access and even remote access to their own parents to allow them to see their grandchildren.

Sharing access to ensure well-being of a child wasn't limited to just infants either. Fiona, an adult interviewee who lives with her mother in a single family home talked about how her mother had access to her outdoor camera even when she was travelling, and this helped her to feel more comfortable travelling multiple days. Fiona also brought up another reason for sharing access to her outdoor cameras, ”Our town is so small, that they don't do announcements. I share the camera so we can see what's going on in the neighborhood.”

On the other hand, there were some notable reasons to not share devices as well. The primary one pertained to privacy concerns, and how data can be misused. Participants across both phases of the study expressed concerns regarding a lack of privacy as a result of sharing, and while they mentioned that even if they only share with people they trust, there may be some data, such as financially sensitive information, that they wouldn't want to disclose. ”I’m not aversed to sharing devices, I’m aversed to sharing information,” said one participant, talking about how important data security is to them.

In addition to this, there was some concerns pertaining to artificial intelligence, or AI. While most devices today are expected to record and store data, the processing of the data is still a topic that made some participants uncomfortable. ”As humans, one of the basic rights we have is the right to change our mind,” one participant said. If sharing devices leads to a disclosure of data, then the use of that data by AI to come up with predictive solutions to force or even influence someone into a particular choice is a major concern.

Other reasons for not sharing devices included potential carelessness on behalf of the other users. When talking about why they don’t share their laptop with their five-year old son, one interviewee claimed ”it’s not about trust. I trust him completely, but I also know that he doesn’t recognize the value of an expensive laptop, and may accidentally break it.”

Yet another reason that participants didn’t want to share technology was due to their desire to not become over reliant on technology in general. Adam talked about how he had grown up without technology and while he admits some things are becoming a necessity in today’s world, he’d prefer to avoid what he can. ”We, as a family have very consciously not gone the Alexa route.” Talking about smart door-locks, he also said how reliance on this can cause issues in case of failure. ”Right now, if I were to get locked out of my house, I can phone a locksmith, and in an absolute worst-case scenario the wait time is an hour or so, and the cost about 500-600 [rupees]. However, if we had a smart lock, I’d have to reach out to the company, they’d have to verify my identity, then send over a licensed professional. That’s at least 3-4 hours outside, and maybe around 3-4000 rupees.”

Some Private participants also talked about not sharing devices just because there was no need to. For example, Henry, who lives alone talked about not sharing devices just because they didn’t have anyone that needed to access the devices. As they live alone, there was no one in the house to share with, and along with a combination of other concerns regarding remote device sharing, Henry mentioned that no one outside his home needed access to his smart cameras, door lock, or TV.

Rather interestingly, reciprocity wasn't a factor for any of our interview participants when deciding whether or not to share a device. All participants were asked whether they expect the person they share their devices with to reciprocate the sharing, and while we expected at least some participants to answer yes, none of them felt that it influenced their decision. ”When I share my devices, I do so to be a good host, and not expecting anything in return,” said one participant. ”If you were to ask me to predict whether the people I share devices with will also share their devices with me, I'd say yes. So in that sense I expect it. However, should that not happen, it wouldn't change my decision to share my devices.”

1.5 Discussion

Following the findings from the survey and interview, we'd first like to reflect back on the Research Questions.

1.5.1 RQ1: How are people sharing smart home device and how does that relate to cultural experience and background?

Looking at the data gathered in the survey stage, it is easy to see how people are sharing smart home devices. The primary devices being shared are those that carry minimal private information, such as TVs, and are generally only shared within the same home or to people visiting the home. Devices such as Smart speakers are also fairly popular, also for similar reasons - they carry limited information. One interviewee specifically mentioned that a large reason they share access and remote access to their personal voice assistant is because they haven't set up any payment information or linked any personal accounts to the device. We suspect that people that tend to link their Amazon account, for example, will be more skeptical when it comes to sharing access, as the risk is larger and financial in nature. People with outdoor smart cameras generally shared access to them remotely, however this was reserved to a very limited circle of trust.

Smart door locks were an example that were discussed with all interview participants to establish a common ground, and the field was split on the topic, with some participants taking about how they'd only share access to people that permanently live in the home, while others mentioned they'd share access to those who enter the home regularly, even if they don't permanently live in the home. This divide was noticeable across the two types of participants we established earlier.

A general trend we noticed was that people we classified under Trusting tended to distinguish between the people they shared devices with, rather than the devices themselves. If the person in question was someone they trusted, they'd be wiling to share any device with them, regardless of whether there was a regular necessity for it or not, whereas if it was people they didn't completely trust, they would not be comfortable sharing any device, even if it meant a little bit of inconvenience.

On the other hand, people classified as Private were more focused on the devices they shared and less so the nature of the people they shared it with. While there still was implicit trust expected from everyone who had access, device sharing was on a need basis, in that even the most trusted people only had access to the devices they needed regularly. For example, Fiona mentioned that while she trusts her mother implicitly and the mother has access to devices such as the smart TV and smart camera, she does not have access to the air purifier and thermostat. This was not due to a lack of trust, but rather a lack of need. Our findings aligned up with that of another similar study, where they found that ”Trust mediates sharing” [TKWRL20].

There exists a strong relationship between sharing practices and cultural experiences, in that all four Indian participants, in addition to the participant of Indian origin that now lived in the US were classified as Trusting based on their responses in the interview. A similar pattern held through for survey respondents that didn't take the interview, as their responses also leaned towards the more conservative side. The three American interviewees that were exclusively influenced by Western (American) cultures all were classified as Private based on their sharing practices.

1.5.2 RQ2: How do cultural differences impact perceptions of privacy as it relates to IoT and device sharing?

Following the results of the study, it is reasonable to conclude that cultural differences certainly impact perceptions of privacy. This is something that all the interviewees, albeit to varying degrees, agreed with. Roughly half said that culture was the primary factor behind their perceptions of privacy and heavily impacted their preferences regarding device sharing, while the other half acknowledged that culture plays a part, but their personalities and the personalities of others around them perhaps played a more significant role.

Fiona talked about how she felt being from Jamaica impacted her upbringing and as a result her views on sharing technology. ”Jamaica is a very small island, and people over there are very private,” she said. ”I was told that your business is your business, and if you go around sharing it, soon the whole island knows.” Her quote provides an insight as to why she doesn't share her devices as freely as some other respondents, and she felt that it is very likely that other Americans of Jamaican descent will have similar views.

David talked about how he felt Indians looked at sharing technology, stating ”We tend to be on the conservative side, but I think it is also because a lot of people that share devices aren't aware of the risks.” His opinion was that if Indians did know the pros and cons of sharing technology, most would err on the side of caution and not share devices, and the people that currently do, do so because they aren't aware of the potential consequences.

An interesting analogy one subject suggested hypothesized placing a person of American culture (more likely to share on a need basis rather than a person basis) in an untrustworthy environment. They said that the same person with the same culture and personality would vary their preferences for device sharing even from location to location, just based solely on the personalities of those around them. This brought up a very valid point that while culture certainly plays a part, it is not the sole contributor to a user's perception of privacy.

To better understand the relationship between culture and the likeliness of a user to share a device, we must look at Hofstede's Insights [Ins]. The figure 1.3 below shows the comparative scores for both India and the USA. The most prominent difference between the two cultures here is Individualism, which is also the most relevant dimension to our study. The United States has an extremely high individualism score at 91, while India is at 48. Hofstede described individualism as ”the degree of interdependence a society maintains among its members,” and the high individualism score indicates that there exists a very low need for interdependence in an American community.

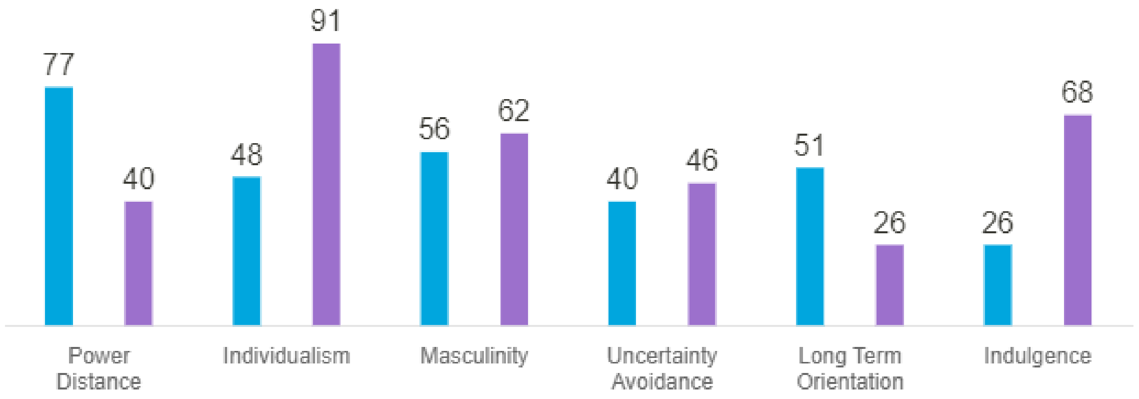

Figure 1.3: Hofstede's Insights for India and USA

This aligns well with our findings as we noticed Indians were more likely to share any device with someone they trusted, even if it did not directly benefit them. Looking back at the Smart TV example, Colin talked about how he'd be okay with someone else in the house using 'his' smart TV even without his permission. His spouse using the TV for entertainment purposes does not directly benefit Colin, however, it does benefit those around him, and this is an example of the communal benefit that can be observed in a culture with high interdependence. On the other hand, Fiona, who owns an external smart camera and uses it to stay aware of happenings in her neighborhood mentioned that she does not share access to the camera with her neighbors, who could also benefit from knowing what's happening around them. This is evidence of the more individualistic approach outlined in Hofstede's theory, where individual goals outweigh communal benefits. Neither of these examples are black-or-white cases given the privacy and security trade-offs that come with them, but the variance in user responses and behaviour is consistent with the expectations based on Hofstede's insights.

1.5.3 RQ3: What features, policies or data flows do individuals of different cultures believe would help or hinder sharing of IoT devices?

In the interview with participants, we also talked about what they felt were some disadvantages of sharing devices right now, or what challenges they faced in doing so. Specifically, participants were asked to describe a negative experience they had when attempting to share a device, and what went wrong. A fairly common theme that participants mentioned was their lack of ability to share just due to their lack of knowledge of and familiarity with the device in question. While most smart devices today have controls to allow for sharing and remote access, these aren't the features that are typically publicized, and as a result, the average user is not aware of how to go about setting these up. Even those who did have basic device sharing set up or remote sharing apps installed mentioned that they were probably not optimizing the use of these apps, and as such, generally more intuitive user interfaces and simpler sharing mechanisms would go a long way in helping increase IoT device sharing.

In addition to this, participants also talked about how the expectations for smart devices is higher compared to their more traditional counter-parts, solely due to the fact that they’re ’smart’ devices. This point is was best explained by Eric, when he was talking about sharing access to the Smart lock. ”If I had a traditional key mechanism, I would give my neighbor or a close friend a spare key, just because there was no other alternative. But with smart locks, you expect more. I’d like to be able to give them access, but would also like to be notified about that access when it’s used, something not possible with a traditional key.” The anecdote shared sums up the enhanced user expectations regarding smart devices perfectly, as they expect features that would not exist if the device wasn’t a smart home device. Talking specifically about policies that would help promote sharing, the ability to only share access during a certain time window or the ability to only share access to certain features are both options that could be extremely valuable. The time window option is something that would help with giving access to house-help, for example, only during the time period they’re expected to be working, while not risking giving them access to the house at night time or during extended vacation periods.

As far features that may hinder sharing, the addition of AI was a stand-out. Like Brian mentioned during his interview, the fact that AI can process all of your data within seconds and create a stereotype for you is extremely scary, and the prevalence of AI in smart devices is the reason he attempts to ”curb the use of technology” where possible and avoidable. This is a sentiment other participants also agreed with, and while AI certainly adds convenience, it brings with it a lot of cons, specifically pertaining to sharing that may strongly dissuade device sharing in AI-enabled devices.

1.6 Conclusion

In this paper, we have examined IoT Device Sharing and Remote Device Sharing, looking at it from a cultural view-point. Our results highlight several factors that indicate a relationship between cultural background and perceptions towards device sharing, particularly the impact of individualism of the culture on the reasons why someone may share a device. Overall, our results indicate that this relationship warrants future work to understand other factors that the sample size off this study may have failed to account for. One important contribution from this study is the two primary types of user groups we identified and classified, based on the devices they own and their need to share given devices.

Based on our findings, we believe that the suggested policies for device sharing and access control may be useful to create better interfaces and help promote device sharing going forward while mitigating the risks that come with it. We contribute our work as an extension of the discussion on the pros and cons of device sharing and the case for remote device sharing and enhanced privacy controls.

1.7 Limitations

We recognize several limitations in the study such as the limited number of only about 35 participants due to resource and cost issues. Given that two distinct cultures were surveyed, we only had a handful of respondents from the cultures to examine, and only eight were chosen to advance forward for the interview stage of the study. In addition to this, the sample chosen was a convenience sample, and is not necessarily the best reflection of either culture as a whole. A large part of the the American audience was recruited from smart home forums and as a result were more tech-savvy and had a greater number of smart home devices compared to the Indians. The survey was also opened to students at the University of Cincinnati, who were generally in their mid 20s, which significantly brought down the average age of the American sample. Of the participants interviewed, two were related to each other and shared similar ideologies for this reason.

In addition to this, there were limitations pertaining to the survey itself. To ensure privacy of the respondent and an opt-in system, participants were allowed to answer anonymously, which could have lead to a single participant echoing their opinion by using multiple replies, however, thankfully this does not seem to be the case. Given that all data was self reported and not observed, any biases a participant carried into an interview or survey would also be reflected in their response. Some partial participant responses were also collected by the survey and if the majority of the survey was filled out, then the responses were used.

1.8 Future Work

Our research identifies what potential sharing features participants desire in their IoT Smart Devices. Working on how to implement our findings into the interface design for new IoT devices could be a potential field for future research. Remote device sharing is a feature with infinite potential and working on making it accessible and appealing to all users could help simplify IoT device management while reducing cloud traffic noise.

Given that this study only examines a small population across two countries, the United States of America and India, future studies could aim to find similar data for a broader range of cultures, better examining the correlation with Hofstede's cultural dimensions. In this study, the only dimension examined was individuality, as the other dimensions between India and the US had similar scores, or were deemed to not directly impact device sharing preferences, but a similar study carried out on different cultures could certainly try and find a correlation between uncertainty avoidance or long term orientation and the need for device sharing.

Further similar studies with larger sample sizes could help eliminate this bias and add external validity through reproducibility.

References

[ABB$^+$20] Dev Agrawal, Rahul Bhagwat, Rajdeep Bandopadhyay, Vineela Kunapareddi, Eric Burden, Shane Halse, Pamela Wisniewski, and Jess Kropczynski. Enhancing smart home security using co-monitoring of iot devices. *Companion Of The 2020 ACM International Conference On Supporting Group Work.*, 1 2020.

[CB17] Victoria Clarke and Virginia Braun. Thematic analysis. *The Journal of Positive Psychology*, 12:297–298, 2 2017.

[CK17] Moonhee Cho and Gawon Kim. A cross-cultural comparative analysis of crowdfunding projects in the united states and south korea. *Computers in Human Behavior*, 72:312–320, 7 2017.

[HGP$^+$18] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Durmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). *27th USENIX Security Symposium (USENIX Security 18)*, pages 255–272, 8 2018.

[Ins] Hofstede Insights. Country comparisions - hofstede's insights. https://www.hofstede-insights.com/country-comparison/.

[MAB$^+$20] Michelle Mazurek, J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Cranor, Gregory Ganger, and Michael Reiter. Access control for home data sharing: Attitudes, needs and practices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 645–654, 4 2020.

[MLK10] Georgios Mantas, Dimitris Lymperopoulos, and Nikos Komninos. Security in smart home environment. *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*, 1 2010.

[SHZ20] Omar Sabri, Tahir Hakim, and Badriah Zaila. The role of hofstede dimensions on the readiness of iot implementation case study: Saudi universities. *Journal of Theoretical and Applied Information Technology*, 98, 8 2020.

[SST18] Roei Schuster, Vitaly Shmatikov, and Eran Tromer. Situational access control in the internet of things. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1056–1073, 10 2018.

[TKWRL20] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter-Lipford. Smart home beyond the home: A case for community-based access control. *Proceedings Of The 2020 CHI Conference On Human Factors In Computing Systems.*, pages 1–12, 4 2020.

[YPY17] Seokung Yoon, Haeryong Park, and Hyeong Seon Yoo. Security issues on smarthome in iot environment. *Lecture Notes in Electrical Engineering*, 330:691–696, 7 2017.

[ZACF18] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *User Perceptions of Smart Home IoT Privacy*, 2:1–20, 11 2018.

Appendix: An Appendix

A.1 Survey

The survey was administered through Qualtrics and can be accessed by using this link