Spring 5-1-2019

A Bystander's Dilemma: Participatory Design Study of Privacy Expectations for Smart Home Devices

Oriana McDonough

A Bystander's Dilemma: Participatory Design Study of Privacy Expectations for Smart Home Devices

A Capstone Project Submitted in Partial Fulfillment of the Requirements of the Renée Crown University Honors Program at Syracuse University

Oriana McDonough

Candidate for Bachelor of
Science in Information Management and Technology
And Renée Crown University Honors
May 2019

Honors Capstone Project in the Information Management and Technology

Capstone Project Advisor: _____
Yang Wang, Assistant Professor

Capstone Project Reader: _____
Deb Nosky, Director

Honors Director: _____
Dr. Danielle Smith, Director

Abstract

Traditional homes have become increasingly filled with Internet-connected devices, turning them into “smart homes.” Currently, research around privacy concerns with smart home devices has focused on the end users. The goal for our research is to understand the perceptions and desired privacy mechanisms from the perspective of a different stakeholder, i.e., the bystanders. Bystanders in this context are individuals who are not the owner or primary user of smart home devices but are potentially affected by the device usage, such as house guests or family members. In order to understand this, we conducted a focus group study with co-design activities to discover bystanders’ perceptions of smart home devices as well as their desired protections and privacy designs. Through seven focus groups with 18 participants, we revealed different bystanders’ concerns (e.g. data sharing) and the factors that affected the bystanders’ perceptions (e.g. device company trust). Using the participants’ desires for the privacy mechanism designs (e.g. awareness of device), we created our own design based on what we learned. Our designs considered the participants’ perceptions and summarized what one should consider when creating privacy mechanisms for bystanders of smart home devices.

Executive Summary

With the exponential growth of smart homes in our lives, we read articles on privacy and security regarding these devices. To our knowledge, the role of the bystander (guest or innocent party) has been overlooked when examining these concerns. Yet the bystander is also a prominent actor, subject to the monitoring, listening, and recording capabilities of these smart tools. This study explores the bystander perspective because the smart home community so far has not been attentive to their experiences and expectations as a non-operator in a home. Bystanders themselves may not be aware of the issues or even of the use of these devices. Furthermore, bystanders face the dilemma of wanting to protect their privacy but also a need to follow social norms by addressing the issue with a homeowner. Over the course of this paper, we discuss this dilemma by understanding bystanders' perceptions and designing privacy solutions to address their concerns of smart home devices.

Table of Contents

Acknowledgements

This study would not be possible without the help of the SALT (Social Computing Systems) Lab, a research group that seeks to understand human interactions with sociotechnical computing systems. They offered the resources and ability for us to conduct the study with participants over the last year. Yaxing Yao, a fourth year PhD student in the iSchool, was an incredible mentor and facilitator during this study. He helped me to construct, organize, and conduct the study with advising along the way. Justin Basdeo is a fifth-year industrial design student at Syracuse University and also assisted me greatly with the study. He put endless time and effort into the study to complete it in the timeframe we needed. Both Yaxing and Justin were huge contributors of the study, so I thank them for their amazing work and assistance.

Advice to Future Honors Students

Find something you are passionate about. This seems like simple advice but after spending months and months working on the same project, it can be very strenuous and exhausting if you aren't working on a project that interests you and motivates you to keep going. If you are working with other people, make sure they are easy to work with and hold you accountable to maintain your timeline. I was fortunate to have a wonderful team to work with that helped keep moving on the progress of the project and keep it interesting and exciting. At the end of the project, you will feel proud and accomplished if you found a stimulating topic and inspiring team that allowed you to create something awesome and worthy of presenting for your capstone thesis.

Chapter 1

A Bystander's Dilemma

Introduction

With the explosive growth of technology in the past few decades, the use of the internet has become a formidable component to developing tools and mechanisms to help improve daily life. Specifically, the Internet of Things (IoT) has allowed devices to become interconnected systems that transfer data over a network. Some devices utilizing this connected system can be defined as "smart home" technology. As defined in previous literature, a smart home "consists of different sensors, systems, and devices, which can be remotely controlled, accessed and monitored"[1]. Users are able to automate, control, and enable features for all types of voice or remote-controlled devices within their homes[2]. Infiltrating households are devices such as smart light bulbs, thermostats, speakers, doors, cameras, etc. which aim to produce efficiency and usability for homeowners.

Because these devices are interconnected and can potentially collect sensitive information, they raise questions about the user's privacy and security concerns[3]. Since smart home devices are used to protect, assist, or enhance users' homes, the devices are physically located within or around the home. This creates a potential security risk concerning what type of

[1] Yao et al., "Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes."
[2] Zeng, Mare, and Roesner, "End User Security & Privacy Concerns with Smart Homes."
[3] Lau, Zimmerman, and Schaub, "Alexa, Are You Listening?"

data is being collected, how long it is stored, and what alternative uses the collected data could be utilized for[4]. Based on other research, these risks could lead to cyber-attacks, data sharing and misuse[5], house invasions based on knowledge of when people are not home[6], and much more. This leaves users exposed and vulnerable when they are not aware and unable to control the security and privacy implications of smart homes within their household.

However, we have noticed that prior research primarily focused either the privacy risks of actual devices or the privacy and security concerns of the smart home end users. There has been little development on other people in the smart home, i.e., smart home bystanders. In this study, we aim to understand more holistically the privacy and security risks that come along with smart home devices by explicitly considering the input from smart home bystanders.

A bystander in the context of a smart home device is defined as anyone who is not the primary owner or user of the device and is either in the same home or visiting a home with smart home devices. Examples of a bystander could be the mailman delivering mail with a smart doorbell, a guest visiting a friend with an Amazon Alexa in their kitchen, or a tenant renting an Airbnb with an Internet-connected security camera. The bystander is different than the smart home user because they have not consented to use this device and may not be aware of the device's functions or capabilities. In the news or other literature, the bystander's perspective is important because an individual may not know their data or privacy is being breached. For example, recent news revealed that a family found a hidden camera live streaming from the

[4] Emami-Naeini et al., "Privacy Expectations and Preferences in an IoT World."
[5] Yao et al., "Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes."
[6] Lin and Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments."

apartment they rented on Airbnb. Moreover, even if they are aware, many times they do not have control of the device to shut it off if they were not comfortable with it.

To shed light on the bystander's perspective when dealing with smart homes, we aim to answer the questions: what are bystanders' privacy concerns? How can those people express their privacy preferences? What factors affect these concerns? How can we protect bystanders' privacy? How can we build systems that combine both end users and bystanders' perspective? And what did we learn from the bystanders' perspectives and concerns?

Related Work

Prior research has touched on the privacy issue in the context of smart home from two levels: the home level, where the smart home was considered as a whole; and the device level, where the research was conducted on one individual smart home device or a network of smart home devices.

On the home level, Zeng et al. conducted an interview study to understand end users' privacy and security attitudes, expectations, and actions of smart homes[7]. Through 15 semi-structured interviews with smart home users or residents, they answered the questions on how and why they use smart home technologies, what are their mental models, what are mitigation strategies already used, and what are design efforts needed? The researchers identified that there is a "mismatch between concerns and power of the smart home administrator and other people in the home" [8]. The researchers developed multiple recommendations for designers of smart home devices by incorporating the concerns that participants found most important to them.

[7] Zeng, Mare, and Roesner, "End User Security & Privacy Concerns with Smart Homes."
[8] Zeng, Mare, and Roesner.

It is worth noting that a smart home contains a combination of complex social interaction, such as the communication between different family members, the surveillance between parents and children, and the potential monitoring of passersby of a home. From a theoretical perspective, the theory of Contextual Integrity (CI) argues that privacy is highly dependent on the context, which further consists of two norms, the norm of appropriate information collection and the norm of appropriate information flow[9]. A person's privacy can be considered breached when either of the two norms is broken. This indicates the importance of understanding the privacy norms in any given context. From this perspective, Apthorpe et al.'s study looked at the privacy norms in smart homes through the lens of the CI theory[10]. Their study surveyed over 1,700 people to discover consumer privacy norms that would enable actionable recommendations to those surrounding IoT devices. The study also discussed the existing privacy norms and how to continue to evolve IoT technology through best practices for device manufacturers. The researchers found many insights into the contextual norms of smart homes that they then recommended manufacturers of devices to use as a way to determine if their device disrupts the established norm [11]. Ultimately the goal of the research was to help design devices that consumers want and feel safe using in their homes by understanding the information flow.

From the device level, Lau et al. looked into voice assistants[12]. Their study focused on the privacy concerns between primary, secondary, and incidental users for smart speakers in their homes. They used an interview method with 17 non-users and 17 users to better understand how

[9] Nissenbaum, "PRIVACY AS CONTEXTUAL INTEGRITY."
[10] Apthorpe et al., "Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity."
[11] Apthorpe et al.
[12] Lau, Zimmerman, and Schaub, "Alexa, Are You Listening?"

to create new devices in the future that considers privacy concerns. They were able to find more information on the users themselves, factors for participant adoption or non-adoption, insight into participants' security concerns, analysis on privacy awareness, why users did not protect or use current privacy controls, and how they would want to improve speakers to handle privacy. They found that "perceived lack of utility or privacy concerns were the main reasons for their non-use," while users considered convenience and setting trends a bigger factor for early adoption than privacy[13]. In conclusion, they recommended design features to provide a more user and privacy-friendly smart speaker such as guest mode, a separate account for children, voice command mute option, incognito mode, etc.

McReynolds et al.'s study focused on connected toys and gadgets such as Hello Barbie, CogniToys Dino, and Amazon Echo[14]. The researchers interviewed parents and children together to find out more about their interactions, expectations, privacy concerns, and desired parental controls for smart devices. They found that parents were very sensitive about the data collected on their children. They were concerned with the toy's recording ability and what companies may do with data they have on their children. The results they found were that parents want stricter parental controls. In order to help improve those parental controls, the researchers provide recommendations for the designers to add mechanisms or controls on the devices to mitigate their children's privacy risks[15].

Building on these insights, Yao et al. conducted a co-design study, trying to explore privacy mechanisms for smart homes by understanding user and non-users' concerns and

[13] Lau, Zimmerman, and Schaub.
[14] McReynolds et al., "Toys That Listen."
[15] McReynolds et al.

involving them in the designing process[16]. Through co-designing privacy-enhancing mechanisms with 25 participants, they discovered six factors that smart home users considered in their privacy designs, including data transparency and control, security, safety, usability and user experiences, system intelligence, and system modality. They then discussed how future practitioners and researchers can use these factors in designing privacy mechanisms. They then discussed how these factors can be used to design mechanisms with privacy concerns in mind.

However, as mentioned in the introduction, prior literature focused on smart home users and thus pointed to the literature gap surrounding the bystanders' privacy perceptions. In order to fill this gap, we conducted a focus group study with various participants to explore different perspectives regarding certain social scenarios we created based on real stories or prior research. We attempt to fill this gap by investigating the certain concerns that bystanders have surrounding smart home technologies and the factors that influence these concerns such as the device manufacturer or the location of the device. We also inspect the expectations bystanders have for different devices. Then by discussing these expectations, we conduct a design activity that expresses certain design factors that the bystander stakeholder considered to protect their privacy from smart home devices. We highlighted the desire for awareness and action through the design mechanisms that the participants' displayed. Lastly, we reflected on the study's findings to address the lessons learned and developed our own designed mechanism based on concerns and expectations. The ultimate goal is to better support different stakeholders' privacy needs in smart homes.

[16] Yao et al., "Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes."

Chapter 2

Methods

Developing Study

As a way to understand the privacy expectations and concerns as a bystander in the context of smart homes, we conducted a participatory design study with a total of 18 participants. We chose to use focus group with different activities as a way to obtain a deeper knowledge of individuals' perceptions. Prior to beginning the study, we obtained Social and Behavioral Research CITI certifications. This is the standard for IRB training, allowing us to properly conduct the research study involving human subjects. The participants were recruited off of Craigslist, word of mouth, and referral. We used a signature flyer and recruiting screen to advertise and understand the individuals' demographics and smart home background. We ran the study with open-ended questions, exercises, and co-design activity. The session was run in our lab for about one and a half hours, and the participants were given $15 for compensation as an incentive to participate in the session. We recorded each session's audio as a way to analyze and conclude results from the participants' responses to the session questions and activities. We also collected all notes and took photos of the exercises as a way to document and include the participants thought process with images.

The study consisted of 18 participants in total over the course of the 7 sessions. The age of our participants ranged from 18 to 78, the average being 40 years old. Nine of the participants identified as female and the other nine identified as male in our pre-session screening. They represented different ethnicities. The participants had various occupations which included roles

such as paralegal, medical student, civil servant, chef, filmmaker/video editor, census bureau employee, university staff, undergraduate students, and retired workers. All of the participants have heard of smart home devices and have experience as a bystander in smart home contexts. Ten of the participants owned smart home devices, five of the participants did not own smart home devices although they have experience, and three participants did not have experiences at all with any smart home devices.

In order to develop a smoothly run study, we ran a pilot study with our colleagues to discover what questions we should ask, what elements worked, and how we can improve the study before proceeding. We had three participants engaged in our pilot study and we conducted it as we would with questions, activities, and the design aspect. After the session, we asked for feedback from the participants about what they thought we could improve on and clear up any confusion in the questions asked or the activities conducted. Based on feedback and observation, we noticed that the participants thought about the smart homes from the owners' perspective, noting that we needed to remind the participants to think about scenarios as a bystander. Second, we noticed confusion with the slide deck, prompting for changes within the slide wording and order. Lastly, the participants struggled to understand what we were asking them to do for the design activity, thus we added in examples of different prototypes such as diagrams, wireframes, and storyboards to assist them with our expectations.

Participant Sessions

As mentioned previously, the study was run with a series of questions and discussion leading up to activities and the co-design privacy mechanisms portion. Using similar questions from previous research [8], we developed a PowerPoint slide deck that asked participants to

introduce and discuss their experience with smart home devices. In order to introduce the bystander perspective, we asked participants to recall the last time they were in the same proximity of smart devices where the participant is not the owner. This allows us to shift the discussion towards focusing on the awareness, concerns, and expectations as a bystander to smart home devices. After reviewing the participants' experience, we addressed our definition of a "smart home" and portrayed examples of smart home devices that we would be discussing throughout the activities. This allowed the participants to all have the same general understanding of what we mean when we say "smart home" in case participants have not had experience with the devices previously.

Following the discussion, we led into exercises which included three activities and one design portion. The first activity we had participants consider different scenarios (e.g. someone else's home or Airbnb) and place cut out photos of smart home devices on a home layout diagram where they felt most comfortable with each device (e.g. in the living room, outside, or not at the house at all). The second activity we had participants place on a scale of comfortability level for each device (e.g. Security camera, Alexa, Smart Toy) where they felt most and least comfortable for the device being located in and out the house (e.g. dining room, bathroom, outdoors). Last, for the activities, we had participants write out their expectations for a scenario as a bystander visiting a home with multiple smart home devices. This activity helped lead into the design portion by understanding possible concerns for the devices based on what participants did not expect of the devices and how they can mitigate those concerns.

For the design portion, we had participants draw and design any type of prototype, app, policy, etc. that focuses on creating a solution to minimize risks or concerns they have with smart home devices as a bystander. This design activity is very open-ended, as participants can design

something feasible or abstract with today's technology. The goal of the design activity is to show the designs and express privacy expectations as a bystander. We discussed and collected all the images that the participants designed. We had participants explain and analyze their designs and other participants' designs to discover what participants were most concerned with and why they wanted to create this design.

Figure 1: Participants designing privacy mechanisms with app wireframes.

Data Analysis

After the sessions were completed, we conducted thematic analysis with the data we collected. We transcribed the audio recordings of the session. The transcriptions were coded and analyzed by three co-authors. This process was done by reading through the transcription multiple times and developing a codebook together. We created the codebook by going through the transcription line by line and assigning the sentences with a sequenced code. After

completing the initial codebook, we individually went through the transcription and compared results. We added and discussed the updated codebook in which we individually completed. We compared our data and the inter-coder reliability of the individually coded transcription was 0.8 (Cohen's Kappa). Next, we used the codebook with more than 100 unique codes to document and organize the rest of the transcribed sessions. Once finishing the coded transcriptions, we were able to develop themes within the data to further analyze the results.

Chapter 3:

Results

Benefits

Although our study focused on the privacy concerns that may arise when adopting smart home technologies, it is important to acknowledge many benefits that also come with it. When conducting the study, our participants highlighted these benefits that smart home technologies create. Such benefits they emphasized was enabled efficiency with daily activity through automation and remote access of the devices. For example, by automating the smart coffee maker to brew coffee every morning or to remotely access your thermostat when out of the house. P5 notes his perspective:

"I think there's a lot of positive stuff that can be done with it. It can make things easier sometimes. Just skipping the step of going on your phone or computer because you can just say it. That is useful. It's faster and that's what everyone wants nowadays." (P5)

Similarly, many participants also noted the benefit of home safety from intruders. When considering the bystander perspective, the participants noted that this can be a benefit when staying at an Airbnb with shared rooms. For example, with an Internet-connected security camera, participants noted that would make them feel more comfortable if staying in a public space.

Bystanders' Concerns

When introducing three different scenarios during the study, participants voiced concerns they had as a bystander observing smart home devices. The scenarios included an Airbnb hidden smart security camera, an Alexa that a family member bought, and a smart toy at a playdate that your child is attending. Although these are just three scenarios out of the many, it helped participants to consider as bystanders their privacy concerns and how they would potentially act in certain settings. We developed 4 main themes for the concerns that participants shared when deliberating the bystanders' perspective. The main concerns were awareness, recording, data collection, and data sharing of smart home devices.

Awareness of Device

Despite the various benefits of smart home technologies presented before, there are also concerns that the participants discussed and examined their privacy as it pertains to the bystander perspective. A major theme in all 7 of the study sessions was the concern for being aware of the devices. Although many of the participants use smart home technologies in their own home,

when it came to other people's homes as a bystander, the awareness factor was an important aspect of maintaining privacy for individuals. The awareness relates to the physical awareness of the device, meaning when they walk into a home, they know there is a smart security camera or Alexa for example. When discussing the difficulty navigating awareness of these devices in another person's home, P8 notes:

"Especially when you don't know you are being filmed. I mean in public places you know you are being filmed at all times. But we never think about it in someone else's home. I think it is more about the home thing." (P8)

P8 mentioned the difference between public to private homes with camera awareness. Since a "home" is considered a more private space, this creates a feeling of security although that may not be the case when a bystander is not aware or familiar with the smart toy. P4 reiterates this concept and also addresses another concept about awareness of the device behaviors or capabilities. She states her concerns as a bystander:

"The Google Home and Amazon Alexa are controlled by awake words, they look like devices. That thing [smart toy], it goes back to the awareness factor. If I walked in, I would never know that is a smart toy. I don't know where it is going, I don't know what it is recording, I don't know if someone knows where my children are. That is when it gets concerning. Because those things like the Google Home and Alexa, people can track where you go. That [a smart toy] gets a child involved. That is where I get concerned as a bystander. I want to be aware of the things." (P4)

P4 was concerned with the CogniToys Dino because she didn't know what it was or what it does. We showed this device as an example in a scenario of a parent picking their child up from a play date to find their kid playing with the smart toy. P4 had experience with other smart

devices but was not familiar with the capabilities or data collection methods of the smart toy, which was cause for her concern.

Privacy from Recording

A second concern that almost all participants had was about being recorded or listened to by smart home devices. Participants expressed their concerns especially as a bystander that they did not know the users' intentions if they had a smart home security camera. They were uncomfortable if the camera was monitored constantly and hoped that it was only for surveillance. In the Airbnb scenario that we showed with the security camera in the living room corner, many participants were not okay with it being there. Although they were uncomfortable with it being there, the participants' action towards the situation varied. Some participants would not stay at the Airbnb, some participants would cover it up or unplug it, while other people argued that it is the Airbnb owner's right to the device, and they would not do anything about it. When presented with the scenario, P5 made a good point about the Airbnb's distinction from a hotel, which has many cameras:

"I mean you think of an Airbnb, you think of it's kind of like a hotel. But it operates a little different. It's like Uber. It's all based in the community. That would kind of freak me out. Definitely. I would be like this is weird. I don't want to stay here. What happens if you want to do whatever you want to do? And there's a camera watching you." (P5)

P5 explained Airbnb as a community environment, where you should feel comfortable staying in another person's home. He was uncomfortable knowing another person in that community could potentially be watching you. After the study, a participant sent a news article

explaining how a family found a hidden camera in the Airbnb they were staying at [17]. The situation was very scary and uncomfortable and with little help from Airbnb, the home owner was not reprimanded until the story went public. There is a reason to be concerned with this type of situation since many times the camera or recording may not be visible. As a bystander with no control of the device, it is even more difficult to navigate this scenario.

When referring again to the CogniToys smart dinosaur and its ability to record sound and respond back to children, P10 was very skeptical of the device:

"There's something about it that doesn't feel right to me about listening to children talk. Like knowing where they are and what they're saying. And it's connected to the internet, so it can be tracked or hacked in some way. So even if it's slightly putting children in danger, I'd be very suspicious of it… I don't know what kind of interactions it is making because it can be inducing some kind of thoughts or ideas. And it can be manipulated in some way. I wouldn't be ok with that." (P10)

The concerns that P10 had were similar to many of the participants. The uneasiness of children communicating with an Internet-connected toy that could be hacked, manipulated, or used in some malicious way. Since the toy is similar to an Alexa or Google Home with voice activated commands and responses, other participants weren't as worried about its recording abilities although because it is a children's toy as opposed to an adult tool was a cause for concern.

[17] Dixon, "Family Finds Hidden Camera Livestreaming from Their Airbnb in Ireland - CNN."

Collection of Information

Another concern from many participants was the possibility of the collection of information to build a personal profile. This entails watching the users' habits of eating and drinking, coming or leaving from the house, purchasing certain brands or goods, etc. This concern is mainly for users of smart home devices, although it can be a bystander concern as well when considering Airbnb, house visitors, or non-user family members in a house with smart devices. Participants expressed their concerns because they did not consent to the device collecting their information. Although one of the less thought of smart device when it comes to concerns, P1 considered the smart fridge a risk due to the collection of information, sharing his perception:

"I just feel like its collecting information. It's got to be going somewhere. Where is it going? I don't know… If it's collecting information about what's in your fridge, then it is building a profile. See that's what I don't like. They all add in together and builds a profile for you and the habits you have. That's why I don't like this stuff." (P1)

P1 highlights the process of collecting information, the unknown realm of where the information is stored or sent, and the collection of habitual data to build a profile. Some participants weren't concerned with this, expressing that individuals' smartphones already do this and that there could be a benefit of positive advertisement toward your needs. Other participants did not like this concept at all, even at another person's house they still have the right to privacy and ownership of their information.

Sharing Information

Similarly, once the data is collected, many participants were more concerned with their information being shared to other sources. P6 and P7 both agreed that this was a concern when it came to maintaining their privacy and companies making money off of them:

"It doesn't really matter which company, the only reason I don't want my data to be extorted like that is I don't want other companies to have that data… they are making so much money off my data so unless they are going to give me a discount or something, they shouldn't be making money off of me." (P7)

"I agree with her I don't think companies should be making money off of your data. I think if you were able to be more selective about what data is sent externally. I think that would be fairer." (P6)

P7 brings up the concern about companies collecting data on them to make money. P6 goes further to suggest that we should be able to control and select which data we share. A lot of participants shared this same perception that they don't want their information shared and don't know what type of information is shared. Although the participants acknowledged that it is probably used for advertisements, they were still unaware of who was seeing the information and using it for their benefit. In a discussion from study session 7 between the three participants about who is listening on the other end of the device and what they are using it for, P17 had a strong statement:

"Personally, I don't think the information should be going anywhere. The only people that should have control of the information should be us. The technology should be used for us to learn about ourselves not for other people to learn about us and we don't know anything. It is all scary, but it is fine. We can't beat it." (P7)

P17 felt that the conversations, actions, or daily routines we do as individuals, should not be used as data for companies to share. He felt we should have control of our information or at least be aware of the information shared, going back to the awareness concern from the previous section. Although the participants admitted they probably wouldn't read it, they suggested a daily report just to acknowledge their data that is being shared without awareness. This would reduce the animosity and apprehensive feeling of not knowing what information is being shared and who it is being shared to.

Factors That Influence Bystanders' Perceptions

The participants throughout the study introduced many concerns that they had with the smart home devices. After analyzing their concerns, we developed 4 main factors that contributed to these concerns. We felt that these factors impacted the perception of the role of a bystander in the presence of smart home technologies.

Company Trust

An interesting factor that was mentioned by a few participant groups was the idea of company trust. In regard to smart home technologies, company trust refers to whether a company is reputable, trustworthy, and has not had any incidents with data breaches or security. For example, if the participant trusts the smart home technology company to seal their data or protect it from server breaches, then the participant would be more willing to feel comfortable using the device. P3 discussed the camera in an Airbnb scenario surrounding this factor:

"At least with Airbnb for me, Airbnb is protecting me when I am renting a place out that is helping me out with acceptance. Airbnb as a company, they can have a house taken down on

Airbnb if something goes wrong. But if it was a sketchy company or finding a house down some dirt road and there were cameras watching, then I would be a little more concerned." (P2)

The perception is that Airbnb is a trustworthy company that would be protecting individuals renting the device to make sure their privacy is maintained. Although that is the perception, there have been many stories where hidden cameras have been found in Airbnb rentals, which an issue Airbnb has to address. When discussing the CogniToys dinosaur scenario, the same issues came up with the credibility of the toy makers. P3 shared his opinion:

"I would be a little skeptical about a company, is it Mattel that makes this toy? I mean Amazon for Alexa they have fail safe after fail safe to make sure their data is secure. I don't know how Mattel makes their server relation… It is kind of like using a cell phone, not an iPhone a smaller cell phone company like is my data really protected on this device." (P3).

Other participants agreed with this perception of data security based on company size and security. If the toy was made from a bigger company or better known for their security to make sure the data is protected on the device, that would allow for the participants to be more comfortable when allowing their child to use the toy.

Device Owner Relationship

Similar to company trust, another factor that affects participants' bystander concerns is their relationship with the device owner. The level of concern with smart home devices varied as it pertained to the relationship with the person that has control of the smart home devices. If the bystander trusted and had a good relationship with the device owner, the concern for the device was a lot lower. If the bystander did not know the device owner very well, or for example was staying at an Airbnb then the concern for the device would be more severe. In the CogniToys smart dinosaur scenario, if the bystander knew the parents of the child more, then they would

trust their judgment for the device. In many of the scenarios also, the bystanders said they would feel comfortable asking the device owner to turn off the device or unplug it. When they didn't know the device owner as much, they would feel uncomfortable asking them to turn off the devices, resulting in more concern for their privacy. As a result, there is a difficult line to teeter about managing your concerns and understanding the owner's rights to the devices within their home. P6 shared his perception with the bystander perspective:

"I mean in one aspect, it may not be best to stop it because when you're an adult and you go into someone else's house or Airbnb, there is a chance where there might be a smart device and if there is one, what can you do if it is not your house? But I mean with my father, I unplug it but with someone else you can't just do it. If I could, I think I would want a way to turn it off. I think I would speak to the parents and ask if they could turn it off for the time being." (P6)

P6 highlights the uncomfortableness when a bystander enters someone else's home and tries to maintain their privacy. When the bystander doesn't know the owner as well, they may sacrifice their privacy because of this uncomfortableness although they may still be concerned. The comfortability and trust of the device owner impact the action taken for bystanders to protect their privacy and react to their concerns.

Location of Device

Since there are many devices with different purposes, where the devices are located also influences the concern that many participants had about smart home technologies as a bystander. The device locations vary throughout individuals' houses, from common spaces to bedrooms to outside. In most cases, the bedroom and the bathroom were the most private spaces. The participants highlighted that they would feel uncomfortable with many devices in those spaces, due to the private nature of their location. We conducted a few activities that looked at the

comfortability with the location smart devices in different scenarios and found interesting results. The more common spaces such as the dining room and living room were somewhat comfortable with devices since they usually had more people in the common area that could distract from the smart devices to threaten individuals' privacy. P9 rationed her comfortability in other people's spaces:

"The more people, the more comfortable. I am comfortable with it in my home because it is mine. If it is in someone else's home, I feel less comfortable. The more private space I want to have." (P9)

Although this may not be factually true, the perception was that when there are more people, the risk of your privacy or data breach is lowered. This rationale also addresses the comfortability difference between one's own home and another person's home. Again, although the devices may be the same in both cases, the perception is that when they are located at another person's house, the bystander is not in full control and may not understand the capabilities.

Specifically, for the smart security camera, the location of the device was extremely important. Most individuals were okay with the device being located outside, saying that it gave them more security and comfortability. When the device was move inside, the comfortability level changed drastically, as many individuals questioned the purpose and abuse of the security camera to be surveilled at all times. P2 had a strong stance when asked about the Airbnb smart security camera:

"I am completely against it. Regardless of where, even if it is not the bedroom. I get what she was saying that you are recorded in restaurants or hotel lobbies. But I am living here for three days. It is more private." (P2).

P2 is against the cameras because it is a home as opposed to a public space. The location of the device, in this case, did not matter. The participants also worried that the cameras may be hidden, such as the news article about the Airbnb we discussed previously in the paper. This brings up a device location of comfortability with devices out in the open as opposed to hidden without knowledge of the device.

Use of Device

Lastly, the perception of the usefulness of the device affects the concern for the participants' privacy. Many participants agreed that they may be concerned about the device, but they also think it is worth the risk due to the device's convenience factor. Since many participants had smart home devices themselves, when it came to the bystander role, they understood that others may have those devices and were okay with it being there since they understood its role. For the Airbnb camera scenario, many participants understood why the owner would have a camera for liability reasons in case something was stolen or broken. Because of this, they were okay with the device and would not cover it up or do anything about it because they felt the usefulness was justified. When considering the smart toys, there was a debate about its practicality and purpose where P16 discusses her perception of this:

"My concern would just be that the kid grows up used to having invasive devices present so I would prefer the Alexa not in the house and the toy not in the house... because I would imagine the purpose of the toy is to get children used to having smart devices and other smart amenities. Personally, I would want my child to be more concerned about their privacy." (P16)

In this case, P16 doesn't understand the purpose of the toy other than having her child accustomed to smart home devices. This would allow for the child to be exposed to data collection and potential privacy violations through the use of smart devices. As a bystander, the

concern comes in when individuals don't understand the device utility and do not find it worth their privacy risks.

Expectations of Smart Home Device Functions

Throughout the study sessions, we conducted a design aspect that began with the participants' expectations of smart home technologies. We had a scenario where the participants imagined they went to a dinner party at a friend's house that had all sorts of smart home devices. We asked the participants to list on one side what they expect the devices to do and what we didn't expect or want the devices to do on the other side. From this activity, we were able to learn about a few themes regarding participants' expectations for smart home devices.

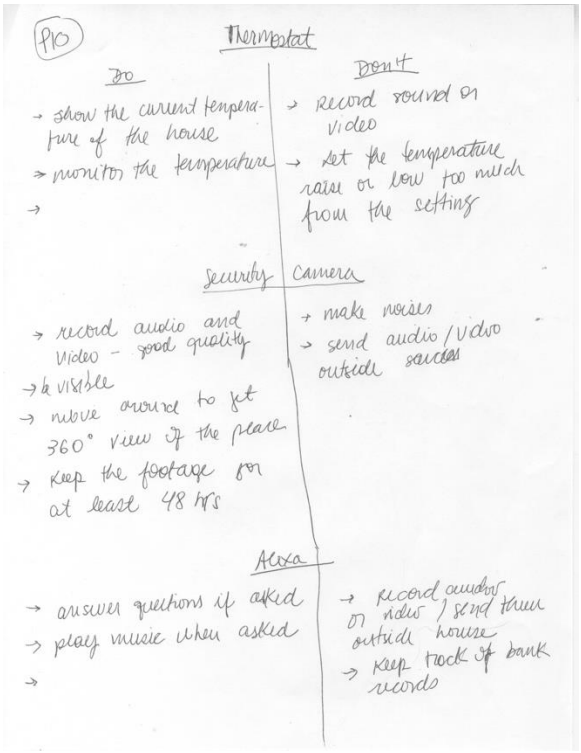

Figure 2: The expectation list by P10.

Bystander Do's

The key concepts that the participants focused on throughout the study were maintaining the expected and designed functions from the smart home devices. The participants expected the security camera to be used for protection, by recording voice or video for liability and sending the recordings to a secure server that only kept the footage for a short period of time. They also expected it to not be hidden and stay stagnant. They expected the Amazon Alexa to respond only with an awake work and answer questions asked properly. They expected other smart home devices such as the thermostat or refrigerator to provide cost-efficient insight such as saving energy with timers.

Bystander Do Not's

On the other hand, the participants listed what they didn't expect the devices to do. This included what they didn't want the smart devices to do such as pick up conversational data, move, make noises, and be used to monitor at all times of the day. They hoped the owners would only use the footage if something was stolen or broken and hoped that it was not used maliciously. As for other devices, the main concept was about not sharing data to outside sources or keep records or audio or video. For the Alexa, participants didn't want audio to be stored from conversations when not addressing Alexa.

Participants' Designs of Privacy Mechanisms

Following the expectations activity, this helped us lead into the co-design portion. By focusing on what the participants listed as what they didn't want the devices to do, the

participants drew up an abstract or practical design of a mechanism that can mitigate any privacy concerns with smart home devices they may have. Overall, the participants' designs were innovative. They had similar concepts, but each added their own aspects and concerns that allowed for us to learn something from what they focused on most. After analysis, we determined the designs were focused on two things: awareness and action.

Bystander Awareness

A constant theme of privacy concerns with smart home devices especially as a bystander is about awareness. Awareness of the physical devices, awareness of the capabilities, and awareness of the purpose of the devices. Many designs focused on this aspect, to make the bystanders aware of what they are walking into when entering another person's house, Airbnb, store, etc. The first step in maintaining individuals' privacy is being aware that there is a risk and minimizing that risk. For example, in the design created by P17 and P18, the bystander would be notified on their smartphone through an app if there is a smart device in your presence. P17 discusses the concept:

"So you are aware of the devices, so you aren't blindsided or secretly recorded or if you don't expect it. And then another caveat is that if any information is shared or has a breach of privacy that you would be uncomfortable with or poses a threat such as your credit card information, it could notify you about that too. I don't know what we would do after that, but it would at least tell you if you are at risk. We were thinking it would be aware of everything and would let you know if it was used for market research or something." (P17)

The design by P17 and P18 focuses solely on awareness and notification of the smart home devices. They wanted to create an alert system that would allow for the participants to be informed of the device presence to make their own decisions about how they want to react.

Bystander Action

Some participants took the awareness factor a step further by creating designs that also included a possibility for action. Action means that the bystander would react to the devices in a way that would include some sort of way to mitigate the privacy concerns they may have. For example, by using an app to ask to turn off smart home devices, control the devices, or trap in the information. One participant created an app that notified exactly where the device is and where to physically move within the house for the individual's audio to not be heard or video to be seen. In the design by P5 from Figure 3, he thought of a social media concept where the users check into each other's house with notification of the devices. There the bystander can select whether they want their audio or video recorded and then it sends a notification to the device owner who can choose to ignore or complete the request.

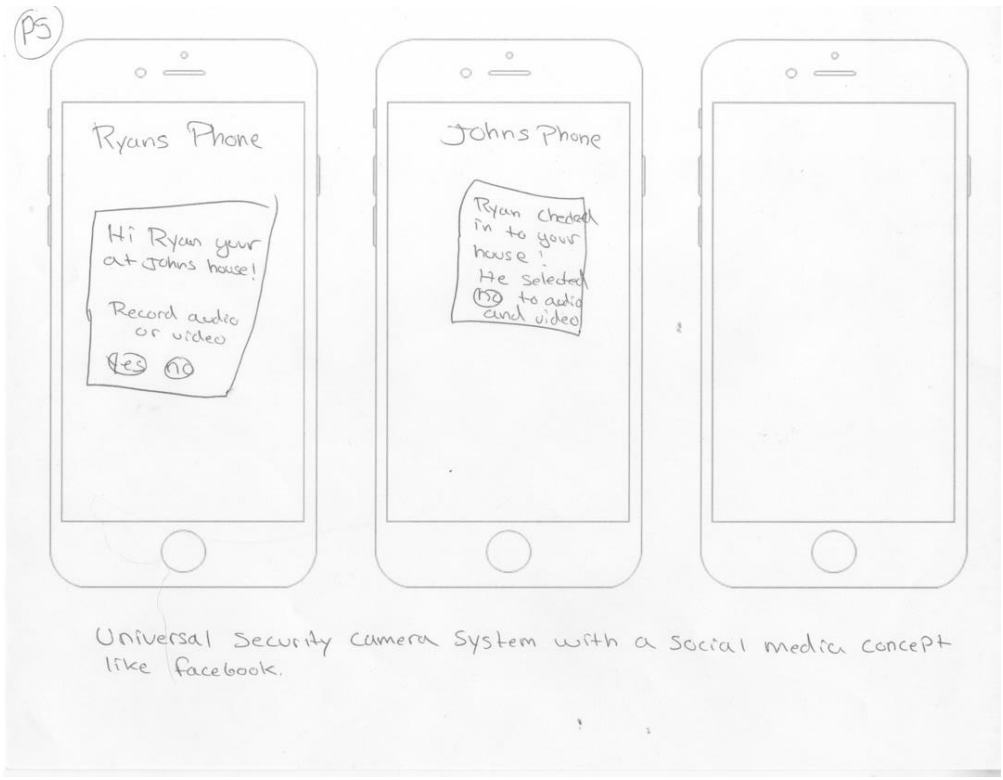

Figure 3: The universal security camera system designed by P5.

In another futuristic concept, P10 created a design that trapped in the collected data inside a certain radius:

"This is a signal blocker that stops information from leaving the house, kind of like bubbles around the house basically. Information can still get in. Signal blocker app will go along with it. I could get a notification that says 'Allow' or 'Deny' information to go out. Potentially it could add other people's devices to your signal blocker or they could share their system with me, kind of like Google Docs 'view', 'view and edit' link share." (P10)

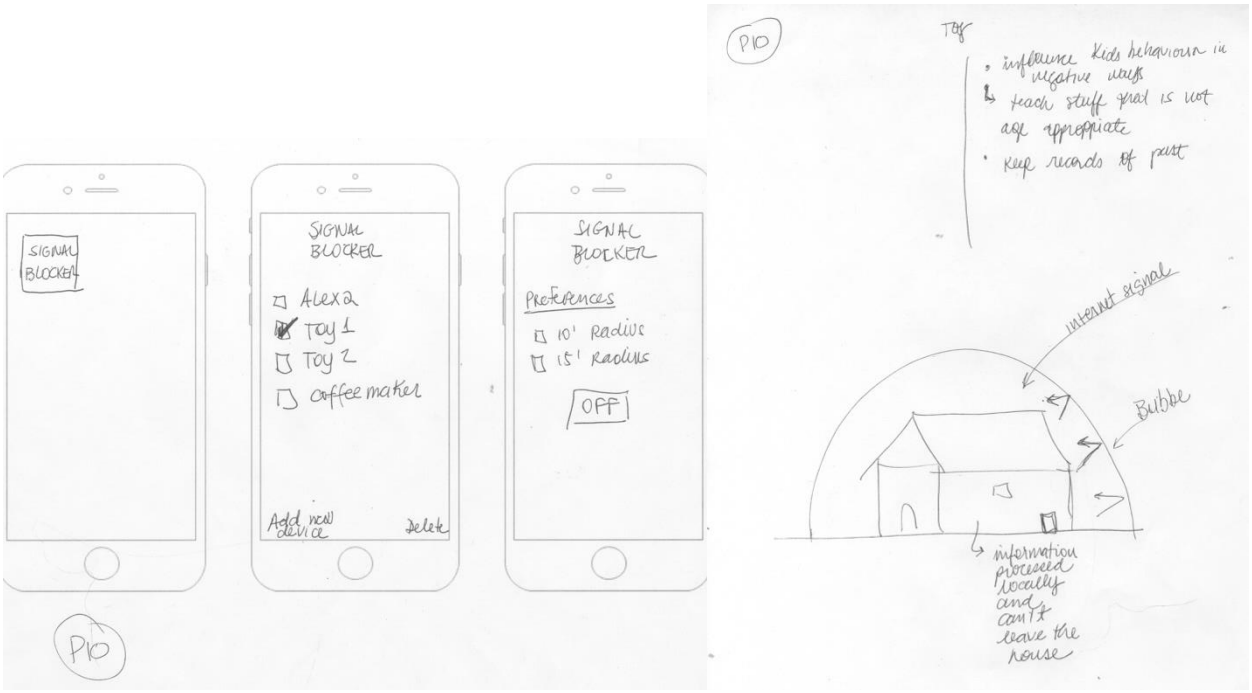

Figure 4: Signal Blocker app by P10.

This design is an app called "Signal Blocker" that selects which devices to block and the range of how far it can be blocked. P10 drew an invisible layer that stopped the information from going outside of the "bubble" that could protect from information leak and sharing. This could potentially limit the collected data inside a house that bystanders could use when attending other homes with smart home devices.

Chapter 4

What's Next

Lessons Learned

With privacy concerns for smart homes becoming a topic of research, the bystanders are easily forgotten when looking at mitigating privacy risks. Throughout this study, we were able to learn a great deal about the concerns, factors, expectations, and wanted changes towards smart home devices and maintaining privacy through certain mechanisms.

We learned a lot throughout the process of creating the co-design study and analysis of the data. To start, many participants had never considered these concerns before. After most study sessions, the participants would mention how the study was very interesting and that it made them think more about the device risks and how to protect themselves. As a result, we were happy to educate people and get them to think about possible concerns they may not have considered before. This allows for them to be aware of their surroundings and knowledgeable on certain vulnerabilities.

Through the discussion and activities, we were able to learn about how people perceived smart home devices and gained insight into their acuities as a bystander. From observation and analysis of the study sessions, we realized that people struggled with their attitudes towards smart home devices as a bystander. Because the device wasn't theirs, it was hard for them to imagine how to control or maintain their privacy. They voiced their concerns but when it came toward action, they had difficulty taking action because they wanted to make sure they were not

infringing on another person's rights and privacy. This was an interesting takeaway and encouraging to know people care about other people's rights as much as their own. They also felt restricted from taking action if this involved a socially awkward confrontation in order to maintain their privacy. This mindset helped many participants create designs that removed that socially awkward interaction while hopefully still considering their privacy as an important measure.

Another takeaway was that participants weren't as worried about their privacy concerns because they considered their smartphone a device that already listened, collected, and shared data. We encouraged the participants to consider their smartphones when designing the privacy mechanism designs to try to stop collecting and sharing data as a whole. By providing the advice that if they were able to provide a privacy mechanism that could protect individuals from all devices, the participants were able to think more creatively about the design portion and provide a unique solution.

When it came to the designs for the privacy mechanisms, the participants seemed to focus a lot of awareness and transparency, sometimes with control for bystanders. This showed us that bystander's wanted to ability to choose how they act when given the transparency on what the device does and how their privacy may be impacted. Having that choice and level of awareness, helps to reduce uncertainty that can alleviate some privacy concerns.

Although participants wanted this type of awareness, the participants also considered how their designs could harmfully affect others if the tools were used by burglars or cause other negative incidents. We would need to look further into solutions and research to determine how this could provide a better tool. If we had more time in the study, we would give the participants

more time to consider more design implications before constructing their privacy mechanisms (e.g. usability, manufacturer, cost, etc.).

Overall, we learned a lot about the bystander perspective towards smart home devices. In the future, we would like to expand upon the scenarios we presented since we limited it to three, yet there are many more to be considered. We would also like to continue with more participants of diverse backgrounds since the experience participants had with smart homes subsequently affected the attitude they had with the devices and perceptions towards privacy concerns.

Our Design

Research done before us suggested the need to develop an understanding of the bystander stakeholder as opposed to the user or non-user. After conducting the study to discuss the bystander role with participants, we were able to formulate a few main themes that lawmakers or manufacturers could take into consideration when creating or regulating emerging technologies. Based on our research that focused on the bystanders' concerns, factors that affect their concerns, and desired ways of addressing them, we generated our own design of how to mitigate privacy concerns through a mechanism that works to combine a lot of concepts that the participants conveyed.

As addressed previously in the participants' design section, the bystanders' focus is on awareness and notification of devices as well as action to protect their privacy through data collection or recording of audio and visual. To further improve this same focus, our design combines the desire to help reduce the social awkwardness of the bystander-owner interaction

yet allows for the bystander to be aware and protected. We created a list of the most important concepts that participants expressed from their perceptions, expectations, and designs. The list addresses six concepts one should consider when creating privacy mechanisms for bystanders.

Participant Design Focuses:

- ◊ **Awareness of Devices**
- ◊ **Knowledge of Capabilities of Devices**
- ◊ **Control of Own Data**
- ◊ **Privacy from Recording**
- ◊ **Ability to Control Devices**
- ◊ **Ease of Interaction between Device Owner**

After considering these aspects, we created a new design based on people's actual expectations and needs. Our design is for a smart device that comes with an app called "Alias Mode" that is used by the bystander and smart device owner. The app would have two distinct features, a notification system for the bystander and an alias mode function that connects to the owner's smart home device.

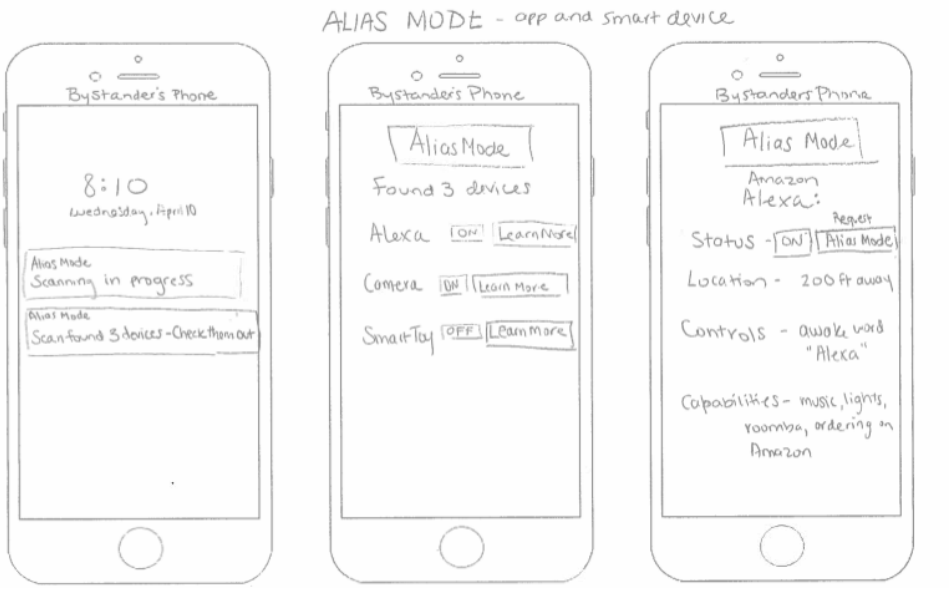

Figure 5: Bystander's Phone with Alias Mode app.

Shown above in Figure 5, the Alias Mode app will scan for devices in the house and list out if the device is on or off, its capabilities, and location in proximity to you. When entering a new

place, it will automatically scan and notify you if they found a device. For example, if a visitor is attending a house party, the app will send the individual a notification when they scanned the house and found 3 devices.

The visitor can then go into the Alias Mode app and see information on the devices. In Figure 5, the visitor clicks on the Amazon Alexa device and can see the status, location, controls, and capabilities of the smart home device. Then they can request "Alias Mode" on the app which sends to the device owner's phone. The app will then connect to the smart home devices where the visitor can request to the owner if they want the device in "Alias Mode," and the owner can accept or deny.

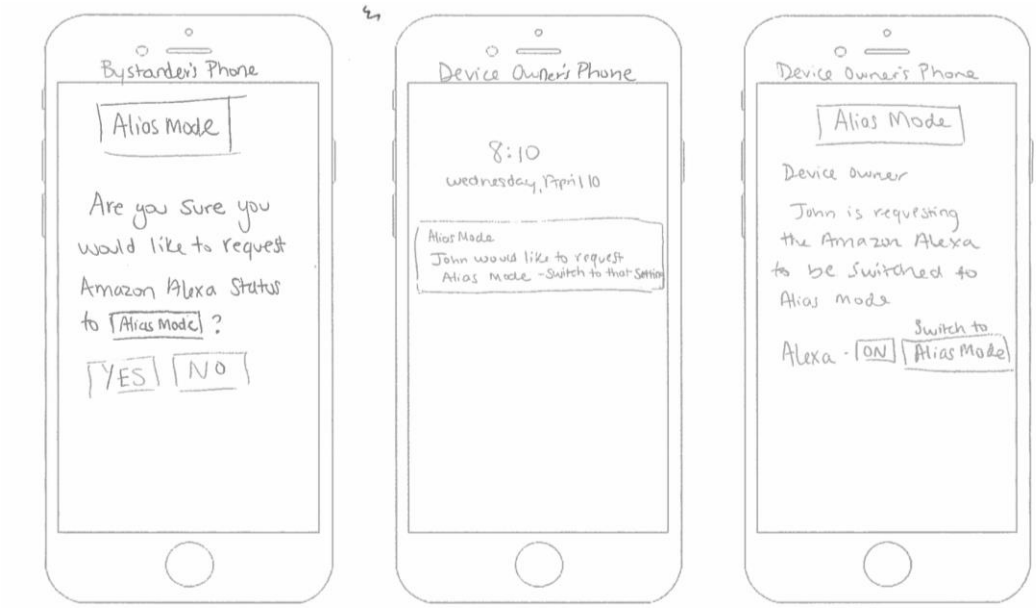

Figure 6: Device Owner's Phone with Alias Mode turned on.

In Figure 6, the device owner will get a notification saying, for example, "John would like to request Alias Mode" with an option to switch to this setting. Alias Mode is a feature on the smart home device that the owner can control from the same app on their phone or from the

physical device. The alias mode would be a setting where the device is programmed to only recognize the device owner's (or designated people's) voice and image. All other people are automatically ignored or generalized as a composite person, such as an alias. As the device learns the homeowner's voice, it will then distort or mask the other people's voices to keep the anonymity of the bystander. Similarly, for a device that captures image, by blurring out the other people's faces the bystander can maintain a confidential identity. For example, if the visitor requests the Amazon Alexa to go into Alias Mode and the device owner accepts the request, the device will now only recognize the device owner's voice. All the other voices will be unrecognizable.

This design would be manufactured by a company that develops the app and smart home devices together, so that they operate seamlessly as one unit. Also, by developing the app for bystanders and owners together, this makes device owners aware that others may be uncomfortable with their device. It also allows for an easy transition to maintain the device owner's right to control while considering others' privacy. The goal for this device is to create a new standard for smart home devices that consider privacy of all stakeholders are important and prevalent.

Before conducting this study, we would not have understood the desires and expectations for privacy mechanisms from the bystander's perspective. Gathering insights on this perspective, we were able to provide an invention of a privacy-centered tool that focuses on different stakeholders and how to release the tension created by device owners and bystanders. We hope that in the future this perspective can be considered more when attempting to alleviate privacy concerns.

Chapter 5

Conclusion

Smart home devices are becoming prevalent in many homes, leaving all stakeholders potentially vulnerable. Previously, research focused on the end users' perspective, leaving the bystanders' perspective understudied. This paper aims to study and understand the bystanders' privacy perceptions through discussion, activities, and a co-design aspect. In the design portion, we illustrated the bystanders' desired strategies to mitigate their privacy concerns. Through seven focus groups involving 18 participants, we were able to grasp a sense of the bystanders' concerns, factors, and expectations concerning smart home devices. We were also able to contribute to the smart home technology community by improving their understanding of the bystanders' perspective for future designs and considering privacy for all stakeholders.

We answered several questions introduced at the beginning of the paper surrounding the expression, protection, and lessons of bystanders' privacy concerns. Our results concluded that the bystander role is significant in the smart home context and their concerns are valid when desiring privacy focused advancements. In addition, we contributed by designing our own inventive privacy mechanism after considering the participants' main concerns and desires. This design focuses on building a smartphone application system and device that combines both end users and bystanders' perspective to incorporate the needs of both stakeholders.

Works Cited

Apthorpe, Noah, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. "Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, no. 2 (July 5, 2018): 1–23. https://doi.org/10.1145/3214262.

Dixon. "Family Finds Hidden Camera Livestreaming from Their Airbnb in Ireland - CNN," n.d. https://apple.news/AZATvGF4pSsuFf_UQhFnu-Q.

Emami-Naeini, Pardis, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. "Privacy Expectations and Preferences in an IoT World," n.d., 15.

Lau, Josephine, Benjamin Zimmerman, and Florian Schaub. "Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers." *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (November 1, 2018): 1–31. https://doi.org/10.1145/3274371.

Lin, Huichen, and Neil Bergmann. "IoT Privacy and Security Challenges for Smart Home Environments." *Information* 7, no. 3 (July 13, 2016): 44. https://doi.org/10.3390/info7030044.

McReynolds, Emily, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. "Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys." In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, 5197–5207. Denver, Colorado, USA: ACM Press, 2017. https://doi.org/10.1145/3025453.3025735.

Nissenbaum, Helen. “PRIVACY AS CONTEXTUAL INTEGRITY.” *Washington Law Review* 79 (2004): 41.

Yao, Yaxing, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. “Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes,” n.d., 12.

Zeng, Eric, Shrirang Mare, and Franziska Roesner. “End User Security & Privacy Concerns with Smart Homes,” n.d., 17.