

# **User Perceptions and Privacy Information in the Smart Speaker Onboarding Process**

by

Gina Herakovic

A thesis submitted in partial fulfillment of the requirements for the degree of  
Master of Science in Information  
University of Michigan, Ann Arbor

2021

Thesis Committee:

Professor Florian Schaub, Chair

Professor Kentaro Toyama

© 2021

Gina Herakovic

ALL RIGHTS RESERVED

## ACKNOWLEDGMENTS

I will be eternally grateful to my advisor Dr. Florian Schaub for his guidance, never ending patience and constant reassurance when my research hit a wall, another wall, and then a ravine. His support and input were invaluable. Thanks also to my friends and colleagues of the Security, Privacy, Interaction Lab (SPI Lab) for their humor, support and willingness to lend a helping hand.

I would like to thank Sean for his steadfast support--you are the love of my life. You still fascinate and inspire me. You influence me for the better. Thank you to my mother whose selflessness, strength and sense of humor made me into the woman I am today. Thank you to my sister, who reminds me to be gentle with myself and that in spite of all its sham, drudgery and broken dreams, it is still a beautiful world. And lastly I would like to acknowledge my father, who shared with me the gifts of education and knowledge, and who gave me the stubbornness to even attempt this thesis.

# Table of Contents

<b>ACKNOWLEDGMENTS</b>	<b>3</b>
<b>Table of Contents</b>	<b>4</b>
<b>Abstract</b>	<b>6</b>
<b>CHAPTER 1</b>	<b>7</b>
<b>INTRODUCTION</b>	<b>7</b>
<b>CHAPTER 2</b>	<b>8</b>
<b>RELATED WORK</b>	<b>8</b>
2.1 Background	8
2.2 Design of Smart Speakers	9
2.3 Onboarding Process Overview	9
2.3.1 Onboarding Processes Can Facilitate Trust	11
2.4 User Concerns & Misconceptions	13
2.5 Behavioral Science In Onboarding	15
2.6 Privacy Notice Design, Informed Consent, and Privacy Controls	16
<b>CHAPTER 3</b>	<b>19</b>
<b>Analysis of Current Privacy Practices and OnboardingFlows</b>	<b>19</b>
3.1 Introduction	19
3.2 Methods	20
3.3 Current Privacy Practices Analysis	21
3.4 Current Onboarding Flows Analysis	24
3.4 Summary	34
<b>CHAPTER 4</b>	<b>35</b>
<b>Design of a Privacy-Conscious Onboarding Flow</b>	<b>35</b>
4.1 Design Rationale	35
4.2 Specific Design Decisions of the Prototype	36
4.2.1 Design Challenges as a Result of Covid-19	37
4.3 Final Prototypes	39

4.4 Demonstration & Explanation of Final Prototype with Privacy-Oriented Voice Commands	43
<b>CHAPTER 5</b>	<b>46</b>
<b>Online Evaluation Study</b>	<b>46</b>
5.1 Online Evaluation of a Smart Speaker’s Onboarding	46
5.1.1 Method	46
5.1.2 Session protocol / instruments	47
5.1.3 Recruitment & Participant demographics	48
5.1.4 Analysis Approach	49
5.1.5 Limitations	49
5.2 Results of the Online Evaluation Study	50
5.2.1. Perceptions of the Onboarding Process	50
5.2.3 Interventions With the Onboarding Design	59
<b>CHAPTER 6</b>	<b>63</b>
<b>Conclusion</b>	<b>63</b>
4.1 Discussion	63
4.1.1 Main Findings	63
4.2 Implications of Privacy-Oriented Voice Commands	66
4.3 Design Recommendations for the Smart Speaker Onboarding Process	66
4.4 Summary	67
<b>APPENDICES</b>	<b>68</b>
APPENDIX A	69
Coding Framework Template for Privacy Practices	69
<b>APPENDIX B</b>	<b>70</b>
Onboarding flows of the Amazon Echo Dot and Google Nest Mini	70
<b>Appendix C</b>	<b>71</b>
Screening Survey	71
Appendix D	77
Usability Test Script	77
<b>Appendix E</b>	<b>80</b>
User Interaction Decision Tree Spreadsheet	80
<b>Appendix F</b>	<b>81</b>

Cognitive Interview Questions

**81**

**References**

**82**

## **Abstract**

User Perceptions and Privacy Information in the Smart Speaker Onboarding Process

By

Gina Herakovic

Chair: Florian Schaub

A smart speaker's onboarding process is extremely important because it is the user's first touchpoint with the device. An effective onboarding process will communicate the necessary information a user needs in order to understand the smart speaker's functionalities as well as how to interact with it. Despite this, the onboarding process has not been a properly considered channel for conveying privacy information to users. This is surprising given that recommendations for communicating privacy information and related privacy controls often include making this information salient to the user and providing instructional use for controls.

In this thesis, I explore the onboarding process for smart speakers as a potentially effective medium for which to convey privacy information. I conducted an empirical assessment of smart speakers' current privacy practices and their onboarding flows in order to determine where privacy information and the communication of this information may be improved. I used my findings from this analysis to develop a smart speaker prototype to test the effectiveness of the speaker's onboarding process in helping users understand the speaker's functionalities. I also designed privacy-oriented voice commands to test within the onboarding process to evaluate if this type of privacy control influences user comprehension of privacy information. The results of this thesis show that the smart speaker's onboarding process can be improved to help users understand the device's privacy practices. Furthermore, they demonstrate that privacy-oriented voice commands show potential for future research despite being ineffective in this study.

# CHAPTER 1

## INTRODUCTION

Fans of science fiction may recall HAL 9000, the artificial intelligence-powered computer assistant accompanying a crew during a voyage to space from 2001: A Space Odyssey [1]. In this story, HAL is able to genially engage with his crewmates through conversational dialogue and playing games--he is considered trustworthy and useful as a result of his ability to fulfill requests made by his human counterparts [2]. While the plot of this story is much more sinister, we are much closer to having our own personal HAL than ever before, thanks to the increased popularity of voice assistant smart speakers within recent years [3]. In a published study from Edison Research and National Public Radio, it has been found that smart speaker ownership has now reached 60 million adults [4]. From smartphones to car stereos to cross-device integration such as in-home temperature control and lighting, these smart speaker devices have become intertwined with our daily lives and habits [5], [6]. The Covid-19 pandemic has further increased this widespread adoption due to stay-at-home orders and business shutdowns [4]. People are stuck at home and in need of entertainment. This has allowed direct access to consumers from companies and third-party app developers behind these voice assistant devices. Oftentimes, users are completely unaware of their smart speaker's data collection practices [7]. This lack of awareness seeps into the insufficient use of a device's privacy settings as users typically do not configure their privacy settings [8], [9]. Moreover, default privacy settings are designed to boost the sharing of personal information rather than securing it [10].

In this thesis, I researched previous work related to smart speakers, user onboarding, and privacy notices in order to understand what prior research has uncovered. I conducted an empirical assessment of smart speakers' current privacy practices and their onboarding flows, and compared my findings from this analysis to those of previous research. I then designed two prototypes of a smart speaker's onboarding process to test the following: the usability of the smart speaker onboarding experience; its effectiveness in helping users understand device functionalities; and how this onboarding experience influences users' comprehension of privacy information and privacy controls. My contributions include the first examination of privacy information within the smart speaker onboarding process as well as design recommendations for a more effective and usable onboarding experience.



## CHAPTER 2

### RELATED WORK

Prior research has examined the individual and collective implications of voice assistant smart speakers and privacy information [10]–[14]. In this chapter, I present related work that analyzes how smart speakers operate and the various ways in which people utilize them. I discuss users' perceptions and misconceptions of smart speakers as well as highlight the potential of privacy notice design and how behavioral science plays a role in these areas.

#### 2.1 Background

Smart speakers are known by a variety of names: virtual assistants, smart home devices, intelligent personal assistants, voice assistants, and conversational agents, among other titles [11], [15]–[17]. While these terms are used interchangeably, it is important to note that a smart speaker is always a voice or virtual assistant, but the assistant is not always a smart speaker. A voice assistant is a piece of software that responds to a user's voice commands or queries such as Apple's Siri or Amazon's Alexa [18]. This assistant can be found in a variety of devices such as mobile phones, cars, buildings, appliances, wearables, and even children's toys [19]–[21]. A smart speaker is a speaker device that contains integrated voice assistant software so that it may respond to commands and perform tasks on behalf of the user [18]. A smart speaker may have a corresponding mobile application; for example a Google Nest smart speaker is connected to the Google Home app. These applications are used to control the speaker along with other connected smart devices that a user may own. A smart speaker may contain more than just an audio playback speaker. It may or may not also include features such as a visual interface display, a touch screen, a camera, smart home hub integration, and more [18].

Smart speakers must be connected to the internet, otherwise they will fail to respond to voice requests because the software within the intelligent device does not handle the queries itself. Rather, it sends the information to a backend cloud infrastructure for interpretation [11]. A wake word must be spoken to trigger the local device for user commands (e.g. 'Alexa' or 'Hey Google') [11], [22]. Once spoken to, the voice assistant will record and pass on the user's audio to voice recognition backend servers, which use a series of algorithms to process the audio and send back a response [11], [22], [23]. The users' speech--including inflection, accent, and context--are all processed and used to determine a response by the algorithms which is then spoken by the voice assistant to the user [12], [24].

Smart speakers are more than just voice-activated speakers. They are devices that can proactively perform tasks on a user's behalf. These conversational assistants possess Natural Language Processing and Natural Language Generation competencies for AI-powered intelligence [11], [12]. They provide users with access to cloud-based services without having to use an interface located on web, mobile, or desktop devices [7]. The true value of smart speakers, however, lies within their hands-free interactions [11], [25], [26].

## **2.2 Design of Smart Speakers**

Smart speakers' functionalities are commonly known as "skills" [12], [18]. Skills give smart speakers the ability to perform a range of user-directed tasks from setting timers to playing music to more advanced tasks such as turning on connected technology such as light bulbs and thermostats. Skills can also be linked together with a single user voice command to perform a programmed routine or series of more complex actions. When invoked, Google's "Good Morning Routine," for example, can adjust connected smart home devices such as coffee makers, and plugs; inform the user of the day's weather and traffic among other daily updates; and then play a selected audio such as music, the news, a podcast, or audiobook [27].

The first skills a user learns are commands created by the smart speaker company, known as first-party skills. Skills can also be created by other persons or organizations, known as third-party skills, through the use of corresponding "kits" such as the Alexa Skills Kit [12], [28]. In recent years, the number of third-party skills have skyrocketed. Google claims to have more than one million skills while Amazon has over 100,000 [29]. While skills can prove to be convenient and useful for smart speaker users, what has proven to be challenging is helping users discover these capabilities, especially given the saturation of available skills. Users therefore need clear affordances to help them discover these skills--otherwise they are not only unlikely to learn and invoke these skills but also unlikely to understand how their smart speaker operates [10], [28].

## **2.3 Onboarding Process Overview**

Typically, a first-time user learns how to interact with a smart speaker through its set up and onboarding process [28]. There is little academic research specifically analyzing smart speakers and how effective their corresponding user onboarding processes. Eriksson [30] examined whether the type of modalities (visual or audio) influenced users' memory retention and feelings in learning how to interact with a smart speaker. He found no significant difference in the type of modality for user remembrance of learnt features [30]. Therefore, to begin this analysis, it is important to define user onboarding

within the human-computer interaction field. User onboarding describes the process that familiarizes new users with the adoption of a product while also increasing the likelihood that this adoption will become successful [31]. Upon the completion of onboarding, a user should be equipped with two things: an understanding of the new product/service's value as well as the knowledge to successfully use the product or service on their own [32]. While there is no set way to design an onboarding process for new users, there are common design patterns used to convey this new knowledge and experience. These patterns include a “tour” (Figure 2.1) which walks the new user through a series of screens that display screenshots and main features; a “setup wizard” (Figure 2.2) which, through a series of form steps, collects a significant amount of information from the user; “dive right in” (Figure 2.3) which allows the user to immediately begin using the product or service while subtly guiding their interactions using cues and nudges; and “annotated tips” (Figure 2.4) which also allows users to get started right away using subtle visual cues for specific features, but in addition, these cues provide tips on how to better use them [33].

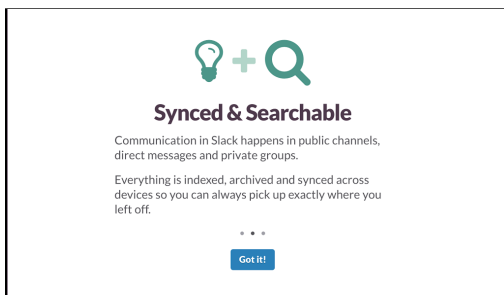


Figure 2.1.

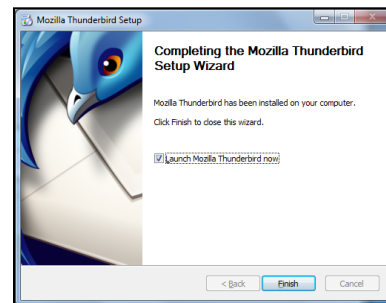


Figure 2.2

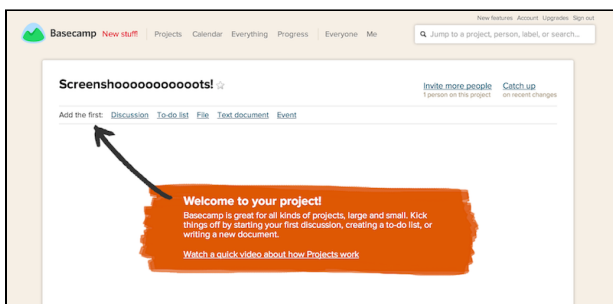


Figure 2.3

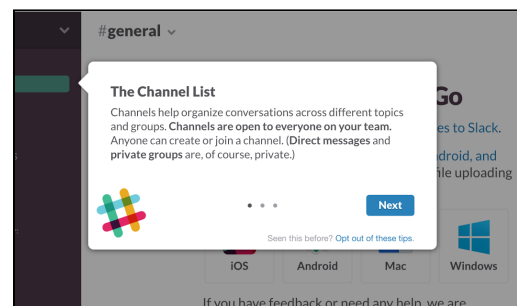


Figure 2.4

An effective onboarding process is crucial for a smart speaker because it sets the new user's expectations for the device and how to interact with it [34]. Furthermore, the functionalities and capabilities of smart speakers are not immediately salient to new users, given their lack of screens, which means they must rely on other instructional means [28], [35]. These types of smart speakers must rely on their onboarding process in order to communicate how the device operates and the ways in which users can interact with it [35]. Moreover, users believe that products should provide usage instructions as this will provide them with sufficient product knowledge [36]. Research has shown that important factors in helping users learn how to effectively interact with a device include both "the availability and effectiveness of training/tutorials" and "the system's ability to actively assist users in becoming proficient in use" [25]. This, in essence, is onboarding. Hakuline et al. [37] examined the effectiveness of an interactive tutor versus a static web tutorial in teaching users how to interact with a spoken dialogue system. Their results showed that users' learning improved more through the use of an interactive tutor. If an engaging onboarding board is crucial to helping users learn how to effectively use a smart speaker, then it could potentially be an area to communicate privacy information and related controls.

### **2.3.1 Onboarding Processes Can Facilitate Trust**

Since the onboarding process is a user's first touch point in engaging with a smart speaker, then this is also a prime opportunity to encourage trust. Michler et al. [38] argue that onboarding and its related information should not be overlooked because it is a factor that helps to build trust between a user and a smart device. This is crucial because research has proven that trust is a major factor in whether users adopt and continue to use smart devices [39]. Instructional onboarding can help the perceived risk and ease-of-use for the device [39], [40]. Additional research has found that in order to effectively understand and use a smart device's security settings, users should be informed of them in the first place [40]–[42]. Thus, if a user is unsure about how a smart speaker functions in relation to their privacy, then the onboarding process is not only a way to quell their concerns and build trust, but it can also be a method to teach them about controls they can utilize to protect their privacy.

In their research on automated aids and human operators, Dzindolet et al. [39] recommend that training information should include appropriate instruction on how to operate the aid and how it functions. Without this, the product can quickly be perceived as untrustworthy and may even fall into disuse [39]. It's important to define the phrase "appropriate instruction." If a user must parse through a complicated instruction manual, no matter if it's physical or digital in form, in order to get their product set up and working properly, then that device is much more likely to be boxed back up and even returned to the seller [43].

Onboarding introduces new users to innovations and makes them aware of their uses as well as any consequences. As such, users should be shielded from product complexities. Brush et al. [44] and Yang and Neman [45] recommend that this be done through a simple, enjoyable user interface that all users can understand without an advanced level of education. Therefore, if a smart speaker's complexities are apparent to the user, then this can affect how a user connects with it. This perceived complexity highlights the theory of innovation diffusion [46] which describes the characteristics of new ideas, products or services, and how those characteristics affect their rate of adoption by societies.

Compatibility, one attribute of this theory, is defined as the degree to which the innovation is perceived as consistent with previous and existing values, ideas, and needs [46]. Oftentimes, compatibility may lead to misuse because of previous experiences and ideas. This is why onboarding is imperative when introducing a new product or functionality of the product, because it can help users correctly adopt and utilize it. If a smart speaker's onboarding process is able to effectively teach the user how to utilize the device then they are more likely to trust it.

Complexibility, another characteristic of innovation diffusion theory, is the degree to which difficulty to understand and use is perceived [46]. In short, the higher the perceived complexity, the lower the rate of adoption [46]. Proactive onboarding, defined as instructing a user on how to use the product, can ease the perceived degree of complexity because it can help users understand how the product functions [31]. This in turn may reduce a user's uncertainty and perceived risk surrounding the smart device [38]. Furthermore, studies have shown that users' intentions to adopt and employ smart devices is significantly determined by whether their understanding of its operating characteristics [40], [47]. Park et al. [47] argue that this is why smart home devices should prioritize their set up and onboarding processes which include the ability to easily connect to the device as well as compatible interfaces (when necessary). If there is a lack of instructional information, then users may rely on trial and error in order to fully understand how to use the device. Previous studies have shown that reliance on trial and error can lead to understanding gaps in functionalities as well as operational capabilities [40], [46], [48].

To better understand patterns of limited interactions with voice assistants, Beneteau et al. [49] studied families' interactions with the Amazon Echo Dot. They found that the families' broad usage of the device decreased steadily over time. Rather than solely relying on manufacturer communications for proper onboarding and learning about the device's functionality, families relied on informal learning through trial-and-error, asking within their network of family and friends, and even asking the Echo Dot about its capabilities [49]. These findings show that the designs of current smart home devices are insufficient to meet users' needs. They also demonstrate the gap in knowledge between user expectations and device functionalities. However, these findings do not address whether the

onboarding processes of these smart home devices played a role in this knowledge gap [49]. This is why it is important to examine how effective onboarding processes actually are in relation to user understanding of both the device and privacy awareness. Additionally, these understanding gaps are not just found in trial and error interactions. Studies have shown that users have incomplete mental models of both smart speakers and privacy risks [10], [12], [13], [50], [51]. This has led to misperceptions and misutilized privacy-oriented behaviors.

## **2.4 User Concerns & Misconceptions**

Users have numerous concerns and misconceptions regarding the privacy and security of smart speakers, as shown in previous studies. These concerns are due to a wide variety of reasons and contexts, including recording private conversations, continued listening even when the device looks to be powered off, device hacking, and the collecting and sharing of personal data [24], [51]–[54]. Abdi et al. [12] found that users actually have different mental models, most being incomplete, of smart speakers' ecosystems. Ecosystems in the smart speaker context refer to how these smart devices collect user information and store and share that data. Interestingly, Abdi et al. [12] discovered that users' understanding of these ecosystems is often limited based on physical and relationship factors. Users tend to see a start and stop line between the physical boundaries of their households, and are typically not aware of data collection outside of their homes from their smart personal assistant.

Additionally, users tend to only consider the vendor of the device and not third parties that potentially have access to their data as well [12], [54]. For example, researchers at Google have concluded that users' inaccurate mental models are a result of the ethereal nature of voice interfaces and their corresponding commands [50]. In addition to showing the impact on user learning, Hakuline et al's study [37] also demonstrated that an interactive tutor can help users with forming more accurate, consistent mental models. In a similar theme of learning, experts have recommended that users should understand the flow of data within a system in order to have a more adequate mental model of how smart speakers work [55]. Experts also generally agree that users' current conceptions of ubiquitous systems such as smart speakers are directly drawn from systems, products, and things that seemed similar [55]. This can help explain why users have misconceptions of how smart speakers actually operate and how to interact with them. If a smart speaker's onboarding process is effective then it will clear up these misconceptions and provide users with a foundational understanding of the smart speaker ecosystem. Therefore, it is important to understand how effective these onboarding processes actually are in a real world setting.

Users' concerns and misconceptions of smart speakers are further compounded within the context of privacy. In exploring security and privacy needs as well as the behaviors of smart home users, Zeng, et. al [10] found limited interaction with privacy and access controls. This could be attributed to several things. Firstly, participants in the study were discouraged by the complexity of the controls themselves because they found the interface to be overly complicated and lacking flexibility especially in regard to onboarding additional guests to the access controls. Secondly, participants did not have a strong desire to use the controls because they were either unconcerned about bad privacy behaviors within their household or they did not feel the need to restrict device access because they found the device to be too mundane and unimportant in regards to their privacy. Thirdly, participants thought the controls would interfere with their desired uses and functionalities of the device. It also observed that users were willing to accept privacy and security risks because of the convenience that smart speakers provided. When given the option, participants decided against setting up a smart device's privacy controls in favor of the utility and convenience tradeoff [10].

Lau et al. [13] studied the privacy perceptions and concerns that influence the adoption and non-adoption of smart speakers by users. They found that, regardless of adoption, people were uncertain about how smart speakers work and whether they were always recording. Those who did not adopt smart speakers due to privacy concerns had high levels of distrust of both the devices and the companies behind them. Specifically, they did not trust companies to comply with their privacy policies and noted that companies can change these terms of service at any time. Furthermore, they expressed concerns over these companies selling their personal data to third parties and their uncertainty with how third parties could use this data. In contrast, the majority of users who adopted smart speakers acknowledged a tradeoff between privacy and convenience. Some users actively traded their privacy while others came from a place of resignation. In order to adopt new technologies, they had to surrender some of their privacy. Those who willingly made the tradeoff stated that they trusted companies to protect the privacy and security of their personal data. However, some users within this group mentioned that companies should be more transparent to skeptical and/or non-users about their data collection, use, and deletion practices [13]. They finished their research with a set of recommendations that may provide more user agency within the context of smart speaker adoption and use. These included designing privacy information especially for resigned users, privacy friendly-default options to build a more solid foundation of user trust in smart speakers, and introducing voice commands as another form of privacy controls [13]. My research will build upon these recommendations to test if they are indeed effective.

Research has also been done on smart homes with multiple residents and the privacy and security risks they pose. Yao et al. [51] used a co-design approach to examine how people conceptualize privacy control mechanisms in smart homes. Participants in the study were directed to design privacy controls for their smart home. They found that participants not only considered their social relationships with others in the same home but they also took power dynamics into account [51]. Similarly, research has shown that multi-user smart speakers can actually cause power imbalances [51], [56]. This is due to the primary user having more in-depth knowledge than a secondary user about the device's functionalities and capabilities [51].

In contrast to manufacturers and third-party vendors receiving private information, Huang et al. [14] conducted a study to gauge users' concerns over smart speakers divulging this information to housemates and other informal entities. Similarly to Zeng et al. they found that participants were aware of the privacy and convenience tradeoff. Yet, uniquely new, participants expressed concern over the uncertainty about this tradeoff-- especially if smart speakers were allowed access to personal data that had not been directly given to the speakers themselves. Furthermore, they discovered that even though users had varying levels of understanding with how smart speakers were sharing information with housemates and visitors, they did have similar strategies for coping. These included avoiding behaviors such as not using specific features of the smart speaker, choosing not to include sensitive information, or putting the device away altogether when guests visited. There was also a variety of accepting behaviors including trust towards both housemates and smart speaker manufacturers, having to helplessly accept the risks because they felt there was no other option, and general laziness in not taking action [14]. This illustrates the varying levels of trust between users and smart device manufacturers, and provides evidence to the knowledge gap of smart speakers' privacy policies and their users. Given that skill discovery is already problematic in helping users understand how smart speakers operate, this will only further compound the privacy problem.

## **2.5 Behavioral Science In Onboarding**

Perceptions and misconceptions of smart speakers do appear by mere happenstance. Schaub and Cranor [69] say it best: "...in practice people's privacy decisions and behavior are rarely rational or predictable but rather highly context dependent and malleable." This is why it is important to also examine theories of human behavior that lends itself to these mental models and decisions. Cognitive load refers to the amount of information that a person's working memory can manage at once. Working memory has limited resource capacity--instructional experiences should be designed in a way to decrease the "load" on a person's working memory [57]. One problem with onboarding users is helping them understand the full functionalities of their smart speaker. They may be affected by a



specific type of cognitive bias, functional fixedness, where their expectations about the speaker's capabilities inhibit the breadth of their voice commands [28]. Yet research has shown that a mixed modal approach of voice-visual smart displays could be a solution to this problem [58]. Displaying features on a screen, such as a corresponding mobile phone app, while still providing users with the opportunity to use commands, could lessen the user's cognitive load--thus allowing them to better understand the device's functionality.

Another type of human behavior that can affect a person's conceptions and misconceptions of a smart speaker especially in regards to privacy is bounded rationality. Bounded rationality is a part of our cognitive decision-making process, and it explains why we choose a decision that is good enough rather than the best and most optimal decision [59], [60]. Moreover, bounded rationality tells us that we are not likely to seek out all information on a given topic because of our cognitive limitations [59]. This is why users might choose a merely satisfactory option over the best one. Bounded rationality can also help explain privacy perceptions and preferences. According to Alessandro Acquisti and Jens Grossklags, bounded rationality can limit our ability to acquire, memorize, and process all relevant information [60]. As a result, we rely on simplified mental models and strategies to help us protect our privacy [61]. These theories are important to consider within the context of onboarding because a user may not choose options that match their privacy, but rather may select a sub-optimal option at the time due to their limited understanding of the content shown in the onboarding flow.

## **2.6 Privacy Notice Design, Informed Consent, and Privacy Controls**

In looking at the onboarding process and its impact, it is also important to review literature on privacy notices and informed user consent. As previously established, users have a variety of perceptions and concerns of smart speakers [10], [12], [13], [50], [51]. This includes their levels of understanding with the smart device's privacy notices and data collection practices. According to Schaub et al [62], the purpose of a privacy notice is, "to make a system's users or a company's customers aware of data practices involving personal information." Moreover, privacy notices should act as a transparent public announcement of a company's data practices in regard to collection, processing, retention, and sharing of personal information [62]. Through this transparency, a user would then be able to make informed privacy decisions. This is where informed consent comes into play. Curren and Kay [63] state that "an individual's consent to use their personal information is the primary means for individuals to exercise their autonomy and to protect their privacy. In order for the consent to be considered 'informed' the user must be able to fully understand the consequences of agreement and/or participation" [64]. Luger and Rodden [55] add an extra layer of complexity with their argument that informed consent should

not be based on a single notification but rather should attempt to reengage and reconnect users over time.

Yet, research has shown that privacy notices and informed consent (also known as notice and choice), or lack thereof, are extremely ineffective for multiple reasons. Privacy notices typically are exceedingly long in length and difficult to understand. Though the content meets legal requirements, it does not meet good usability standards. As a result, these systems are unable to connect with their users in a meaningful way [65]. Users rarely read through the entire notice and usually ignore it altogether [19]. These notices are saturated with legal and technical jargon that buries any information related specifically to user privacy [65]. Furthermore, they typically do not meet the standards of the Fair Information Practice Principles. Originally developed in 1980 by the Organisation for Economic Co-operation and Development (OECD) and again updated in 2013, these principles promote privacy as a fundamental value and provide practical recommendations for privacy implementation [66]. When a notice is full of legalese and lacks good usability, it violates the principles of Collection Limitation and Openness. This is because a user is not being made readily aware that their personal data is collected and the main purposes for this collection. As a result, they are unable to wholly consent because they do not have the full knowledge of this data and privacy practices [66].

The timing of notices also has a significant impact on their effectiveness [62]. This is particularly significant when examining onboarding processes because if a privacy notice is presented at an inopportune time, then a user is more likely to ignore it rather than shift their attention away from setting up the smart speaker in order to read through a lengthy notice. Privacy notices can cause a neurological habituation effect where users quickly click through and agree without considering what their consent entails. Any type of warning or risk is literally not registered in the user's brain due to the repetitiveness of the notices.

System constraints such as limited screen real estate and various interfaces including input and output modalities, along with the context of ubiquitous computing, have impeded privacy notice design [62]. When a device lacks a screen or user interface display, it is exceedingly difficult to add in privacy notifications and settings that are clear and easy to find for users [67]. As a result, and what is arguably more important, these constraints and contexts have lessened user agency in allowing for and providing informed consent [55]. In discussing design implications for voice assistants and smart speakers, Ammari et al [68] discuss how critical it is that developers of these smart voice devices provide usable and prominent privacy notices especially in regard to informing how users have control over their personal data.

Privacy notices and consent choices that lack good usability standards can result in the previously discussed misconceptions. Users may have inaccurate assumptions about the company or product because they are uncertain about the data practices [13]. They may assume that the company is engaging in practices that they find privacy invasive, such as selling their information to third parties or listening to their conversations [13]. When users discover that these practices are not aligned with their expectations, they can experience a nasty surprise. Schaub & Cranor discuss how users learning that their personal data had been harvested without their knowledge in the Cambridge Analytica scandal led to Facebook being slapped with the largest regulatory penalty to date [69]. As such, it is in a company's best interest to properly inform their users of unexpected data practices as well as highlight the choices users have in controlling their personal data.

These privacy-related controls should properly convey both the options a user has as well as the potential consequences of their choices [69]. For example, when checking a box or clicking a button to opt in to share device stats and crash reports with developers, the user should understand what device stats and crash reports actually mean, what specific information is being shared (e.g. if the stats are anonymized), and for how long that information will be used and stored. Similar to data practices, the company should also share unexpected ways a user can control their personal data. Amazon now allows the use of voice commands for users to delete their voice recordings on Amazon smart speakers, for example. A user simply has to say, "Alexa, delete what I just said" and the speaker will remove that voice recording [70]. However, these types of controls might not be obvious to users especially those who are novice smart speaker owners. By properly communicating data practices and conveying privacy controls, companies have the opportunity to build trust with their users. These efforts can demonstrate to users that the company cares about and is interested in protecting individual privacy [69]. A well-designed onboarding process could be the place for this type of privacy communication.

## CHAPTER 3

### **Analysis of Current Privacy Practices and Onboarding Flows**

For this thesis, I designed a two versions of a smart speaker prototype to test the usability of its onboarding experience and to answer the following research questions:

1. How effective is a smart speaker's onboarding experience in meeting users' expectations and helping them understand device functionalities?
2. Furthermore, how does this experience influence user comprehension of privacy notices and controls to facilitate trust between the device and the user?

In order to answer these questions, I followed a user-centered design process to design and test a smart speaker's onboarding experience and its privacy notices. This process consisted of three systematic phases: analysis of current smart speakers and their company's privacy practices, design of a smart speaker's onboarding with a privacy-informed intervention, and evaluation of the onboarding and developed intervention. In this chapter, I describe systematic analysis I performed to evaluate current privacy practices and onboarding flows of smart speakers.

#### **3.1 Introduction**

Currently, the literature lacks studies that specifically evaluate the effectiveness of smart speakers' onboarding processes, especially as they relate to users' awareness and understanding of privacy. Prior work has identified commonalities of mental models surrounding both privacy and smart speaker ecosystems. However, no formal, published evaluation has been conducted to study the ways in which a smart speaker's onboarding process affects users' perceptions of privacy and their awareness of privacy controls.

My research builds upon this past work by analyzing the onboarding flows of two popular smart speakers (the Amazon Echo Dot and the Google Nest Mini), and how these flows communicate their respective company's current privacy practices. Through this analysis I found that current privacy practices do not meet good usability standards because they are saturated with legalese and are exceedingly long in length. These issues are further compounded by lack of screen real estate because these smart speakers do not have a graphical interface but rather must be set up through their corresponding mobile applications. Additionally, my analysis revealed that current onboarding flows are extremely lengthy and do not properly convey information regarding privacy or related controls.

## 3.2 Methods

My analysis began with carrying out an empirical assessment of Amazon and Google's data practices and the corresponding notices. I chose these two companies because together Amazon and Google dominate more than 50% of the global smart speaker market [71]. Moreover, they also provide some of the cheapest smart speaker options on the market, with the Amazon Echo Dot and Google Nest Mini both priced at \$49 [72], [73]. This market saturation combined with budget-friendly options makes it highly likely for consumers to own one of these two devices. My goal with the empirical assessment was to analyze what information each company provides on their data and privacy practices within the context of smart speakers, and how they are communicating these practices to users. Do they provide choices to their users? How specific is this information? Are they acknowledging any risks? What privacy controls, if any, are made apparent to the user? I wanted to examine what information users might find unexpected about these practices as well as what risks they may pose to users.

To conduct this assessment I created a coding framework [Appendix A] where I aimed to answer the same set of five questions for each notice. The questions were employed because they allowed me to examine how these companies are communicating their privacy practices to users, how specific this information is within the notice itself, and how instructional these notices are in providing choices and controls. Additionally, these questions helped me identify what information I think users might find unexpected about these practices. I would use the answers to these questions, specifically unexpected practices, to inform my prototype design in Chapter 4. I obtained these notices by parsing through Amazon and Google's company websites and selecting notices that mentioned data, privacy, and/or their smart speaker devices. Rather than continually checking Google and Amazon websites each time I parsed their notices, I uploaded each one into a Google Doc with a note at the top recording when the notice was last updated. It was important to keep track of when I accessed these documents and when they were last updated because a company can make edits and changes at any time, and I did not want my analysis to suddenly shift because Amazon or Google updated their notices. The results of this analysis are discussed in Section 3.3.

After completing this examination of privacy notices, I then analyzed and mapped out the onboarding flows for both the Google Nest Mini and the Amazon Echo Dot. This consisted of purchasing both devices, then setting them up and going through their onboarding processes. In parallel, I recorded every subsequent piece of information provided by these two smart speakers through screenshots and video recordings. I made these recordings so that I could refer back to them whenever privacy was communicated, and as a point of reference for when it came time to design my prototype in Chapter 4.

I closed out this mapping by aligning where privacy information found in current privacy practices matches within the onboarding flows.

My goal for this analysis of current onboarding flows was to first see how these flows are organized and then to identify any potential deficiencies where privacy information is integrated. It was vital that I personally experience each company's onboarding process so that I could understand, from a novice smart speaker user perspective, what and how privacy information is being communicated. As a UX researcher and designer, I also needed to critically assess the overall user experience of these onboarding processes. The results of this analysis are discussed in Section 3.4.

### **3.3 Current Privacy Practices Analysis**

Over the course of September and October 2020, I read through and analyzed 46 notices relating to the Google Nest Mini [Figure 3.1] and 24 notices relating to the Amazon Echo Dot [Figure 3.1]. This mapping out of smart smart speakers' related privacy notices also facilitated the creation of a high level overview across a vast number of documents. In addition to examining how these notices fit within a smart speaker context, this mapping also allowed me to see the parent-child relationship between notices and where notices overlap such as device FAQs. I performed a word count of all notices related to the two smart speakers. The Amazon Echo Dot had a grand total of 43,064 words. To put this into perspective, 46,000 words equates to about 86 single spaced pages or 172 double-spaced pages [91]. A typical document with this long would be a short novel or other published book. The Google Nest Mini had a grand total of 51,733 words. A word count of 50,000 equates to about 100 pages single-spaced or 200 pages double-spaced pages. Typical documents that are 50,000 words or more include full-length novels [91].

I determined which privacy practices are unexpected through two main ways: first, is through my own novice perspective. I have never owned a smart speaker device so I noted which practices I found most unexpected such as the company collecting your contacts' information through your mobile phone's phone book. Second, I performed internet search queries such as "What do I need to know about the Amazon Echo?" or "unexpected privacy practices Google smart speaker." I then looked through internet form, namely Reddit and Quora, to see what other types of questions people had regarding smart speakers. I used my own notes along with my internet research to then get a baseline understanding of what users find to be most unexpected. It was surprising for me to learn that many users found rather basic privacy practices to be unexpected. Most of what I found was not incredibly advanced but users still did not expect these practices. This included the types of information collected

such as biometric data and connected app and device collection such as the previously discussed mobile phonebook.

My analysis of current privacy practices demonstrated previous research's findings: privacy notices lack usable, transparent information as a result of exceedingly long documents, complex legalese and technical jargon, and a lack of forthcoming information regarding privacy choices and controls [62], [65], [69]. Placing this within the context of smart speakers, these notices become even more ineffective due to screen real estate. Since the Google Nest Mini and Amazon Echo Dot lack screens, they must rely on their corresponding mobile applications which further constrain a user's ability to quickly find answers to privacy questions they may have about their smart speaker.

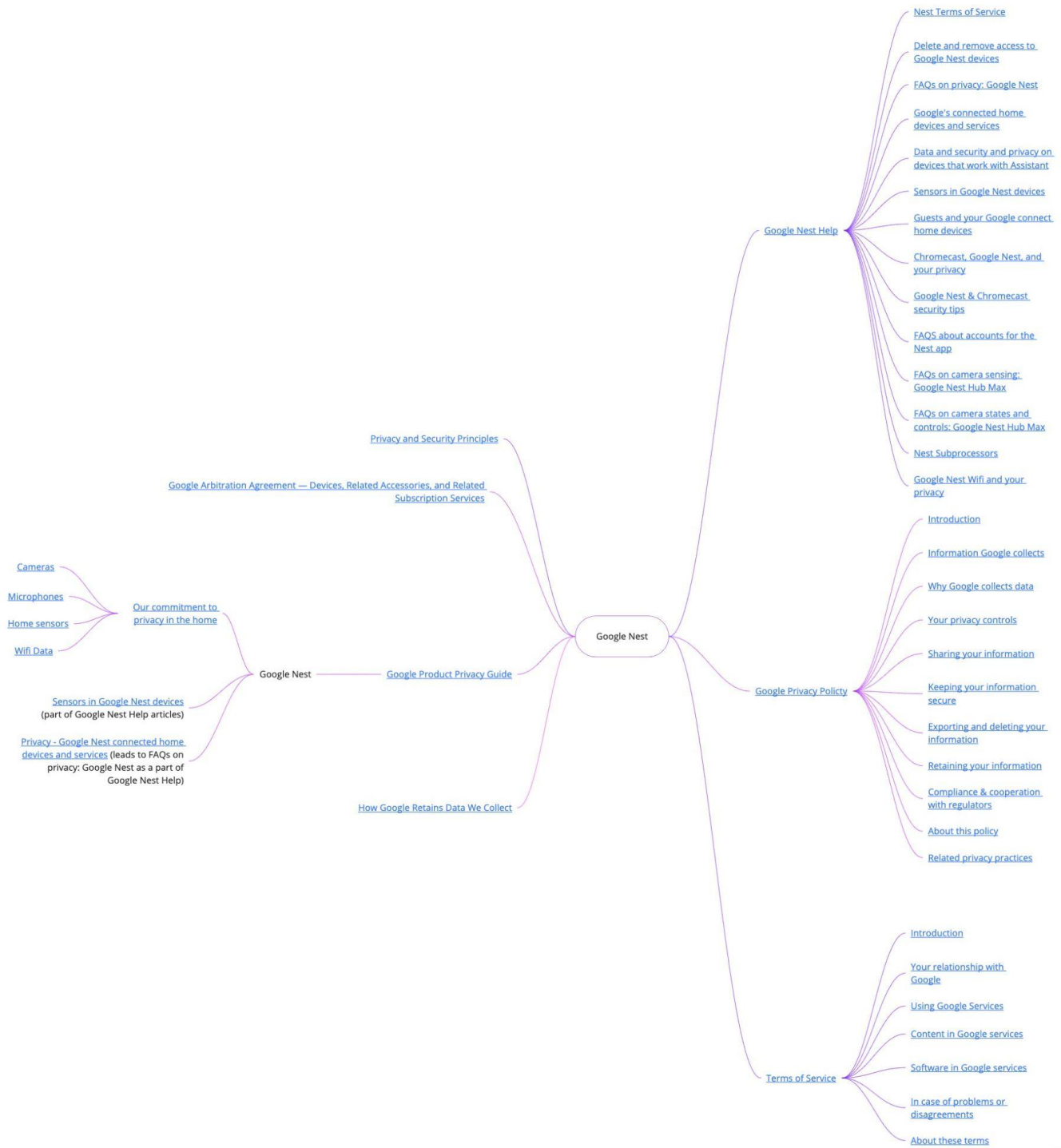


Figure 3.1: Google Nest Mini Privacy Notice Mapping



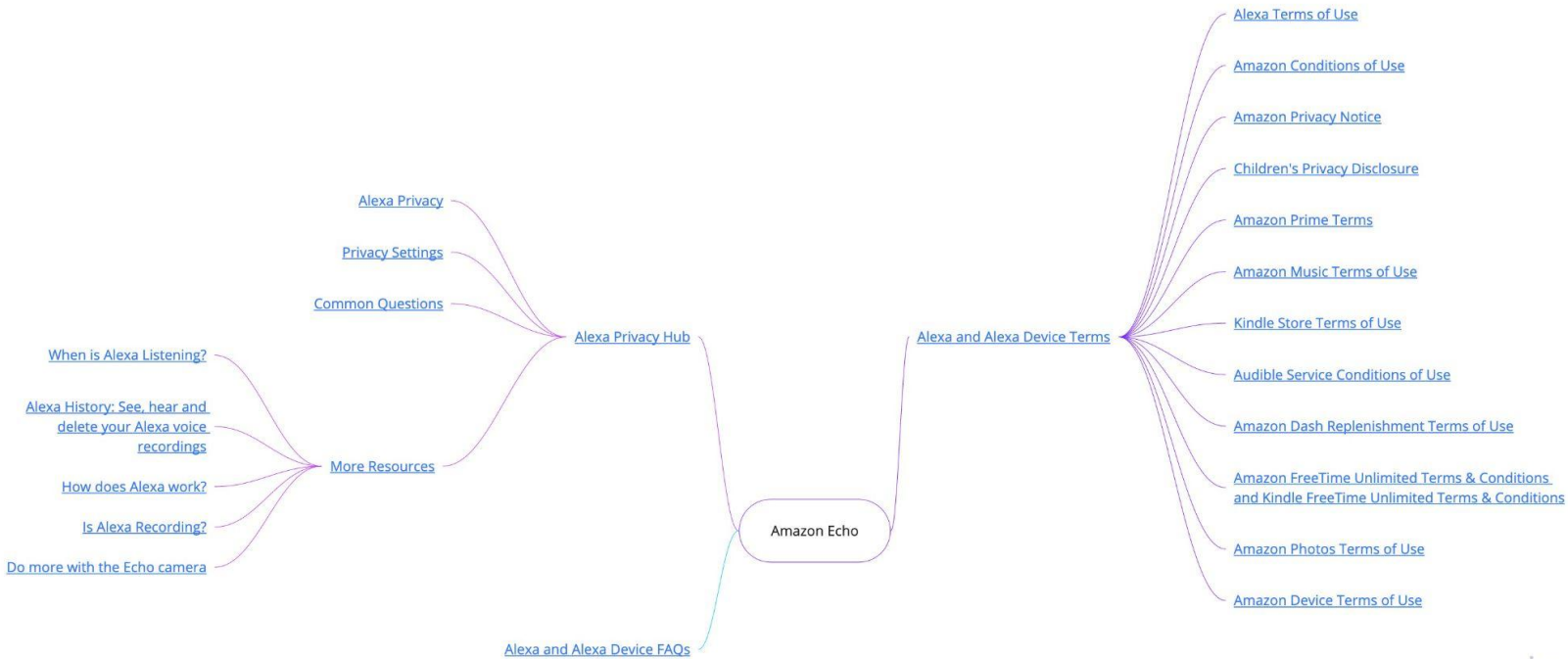


Figure 3.2: Amazon Echo Dot Privacy Notice Mapping

### 3.4 Current Onboarding Flows Analysis

Only the Amazon Echo Dot provided supplemental information in the form of an email following the point of purchase [Figure 3.3]. I found the privacy control information listed “Designed to protect your privacy,” to be vague. The image of a microphone with the red slash through did not signify to me that I can control the smart speaker and prevent it from listening to me. Furthermore, I found that the use of “microphone controls” did not actually tell me where these controls are located or what these controls actually do (e.g. whether they mute the speaker or prevent guests from talking to the speaker). I also found “delete your voice recordings” to be unclear. Again, this information does not instruct me on how to specifically do that or what the effects are of an action like this. While this was only an introductory email and not meant to teach me how to use the device, I did find similar vague language and casual mentions of privacy controls within the onboarding flows.

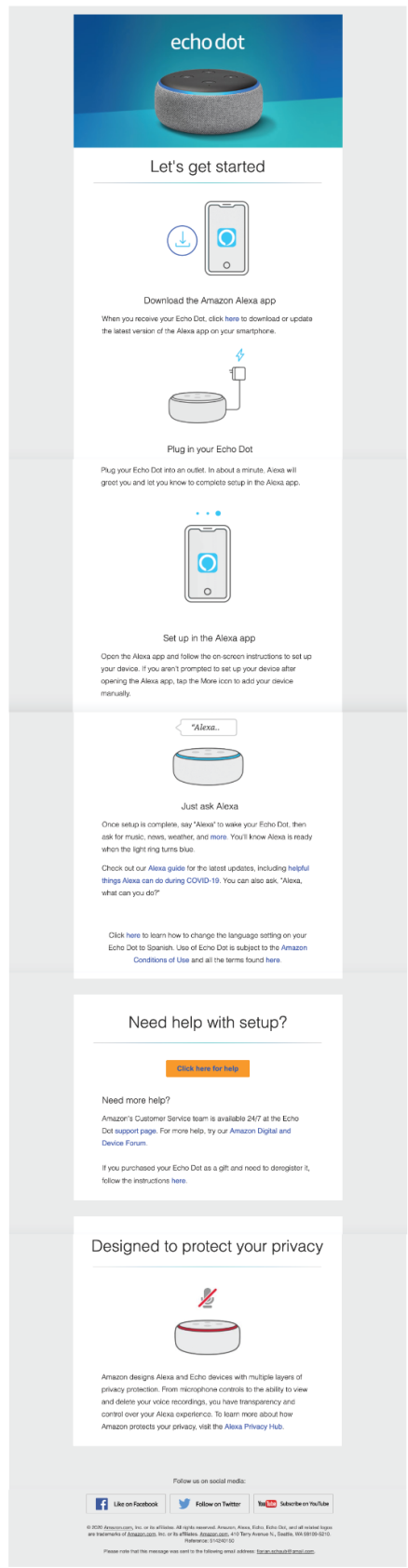


Figure 3.3: "Welcome to Echo Dot" Amazon email

Both the Google Nest Mini and the Amazon Echo Dot have corresponding mobile phone applications: the Google Home app and the Amazon Alexa app. These apps must be downloaded on an external mobile or tablet device in order to fully set up the smart speaker. It is within these apps that the majority of the onboarding takes place. I found the onboarding process for both smart speakers to be long but what was shocking to see was that the Google Nest Mini's onboarding had almost twice as many screens as the Amazon Echo Dot [Appendix B]. In total, the Amazon Echo Dot had 42 onboarding screens, while the Google Nest Mini had 73. What was even more surprising was how long it took to even begin interacting with the device itself. These interactions would eventually include tapping the device, speaking to it, muting the microphone button, looking for lights, etc. The Amazon Echo Dot allowed me to interact with the speaker about halfway through the onboarding process, and only after I had agreed to their terms and notices. It took even longer to begin interacting with the Google Nest Mini device. I had to get about three-quarters of the way through, again agreeing to terms and conditions and arbitration agreements.

Within the Google Nest Mini onboarding process, there were 5 screens related to third-party services and sponsored posts [Figure 3.4]. In hindsight, this should not have been surprising, given that the majority of Google's revenue is through advertising [74]. These marketing screens and nudges towards third-party services brought Lau et. al's [13] research to mind. Their research found that users had concerns over smart speaker companies selling their personal data to third parties, and how these third parties would use this data.

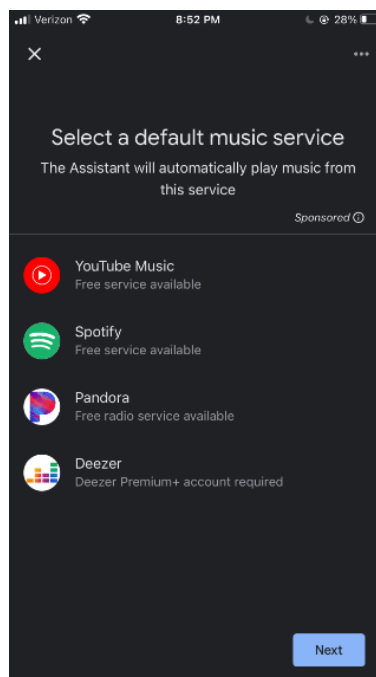


Figure 3.4.: Screenshot of a sponsored post for Google and additional third-party services

As previously discussed, the onboarding process could be a way to soothe these types of concerns. However, the Google Nest Mini’s onboarding almost does the opposite because when the “Sponsored” text is clicked on, a new external browser pops up with a link Help Article [Figure 3.5]. This article does not provide any specific information regarding who exactly Google’s service partners are, if and/or how these partners use data collected by the Google Nest Mini, and if Google sells personal information collected by the smart speaker to these service partners.

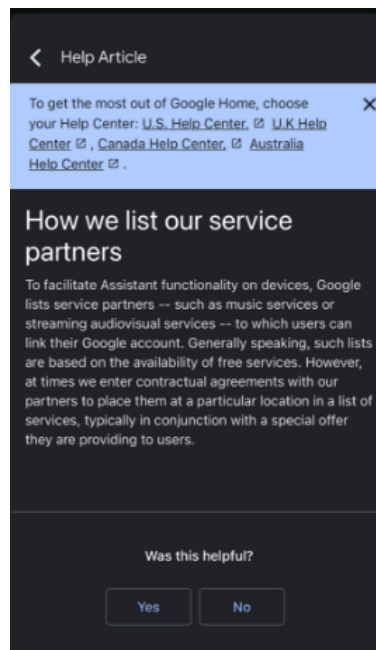


Figure 3.5: Screenshot of Help Article regarding Google’s Service Partners

In order to understand the various contexts in which users adopt and use the device, I had also tested out five different scenarios: setting up the smart speaker without a company-related account (e.g. an Amazon account); creating an account in order to set up the smart speaker; setting up the smart speaker with a previously made account; connecting to a third-party application during the mobile application onboarding; and a secondary user (someone who would not be the primary user of the device) trying to use the device. With both devices, I was unable to set up the smart speaker without a Google or Amazon account. I was intrigued by this mandatory company-related account information, specifically for Google, because it seemed possible that they were trying to nudge me, as the user, into account creation. This nudging felt similar to the third-party services I previously discussed.

My analysis also found three different types of privacy information that I encountered during both onboarding flows. The first type was “informational,” meaning when and where did I encounter material that was purely informational without any related actions (e.g. a screen that tells or describes information to a user without requiring their consent) [Figure 3.6]. The second type was “choice/opt-in,” which referred to any time I had to make a choice such as agreeing to a terms of service notice or opting in to saving my audio recordings [Figure 3.7]. The third and final type of privacy information was “privacy control.” This was for any provided information that informed me of controls relating to my privacy such as a mute button [Figure 3.8]. Some screens could be a combination of privacy types such as having both informational text and a choice about privacy [Figure 3. 7].

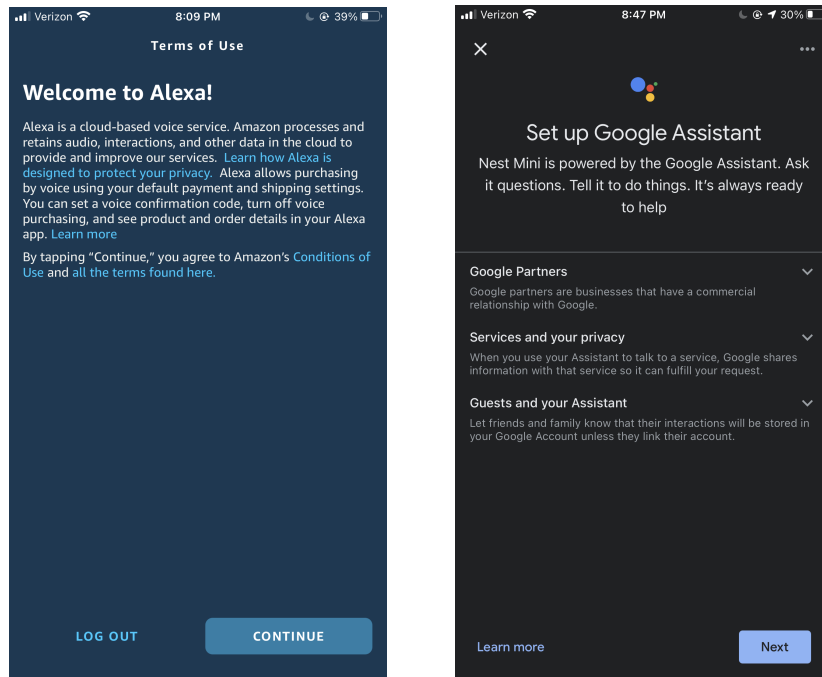


Figure 3.6: Screenshots of informational privacy in the Amazon Alexa app (left) and the Google Home app (right)

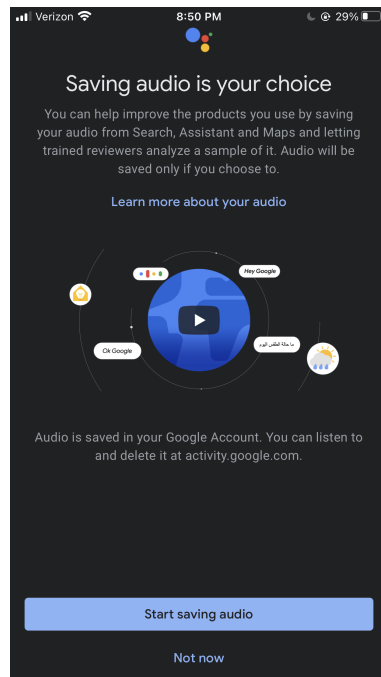
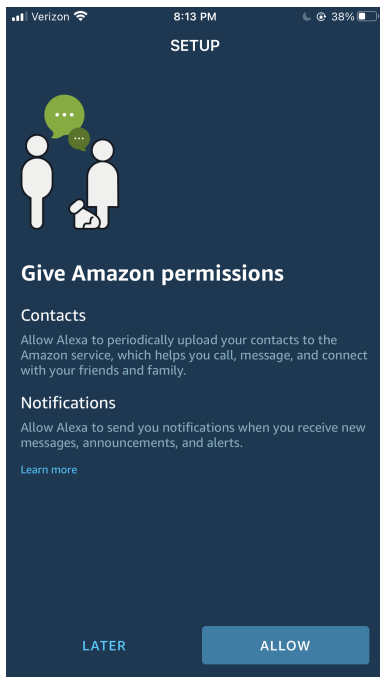


Figure 3.7: Screenshots of choice/opt-in privacy and informational privacy in the Amazon Alexa app (left) and choice/opt-in privacy, informational privacy, and privacy control in the Google Home app (right)

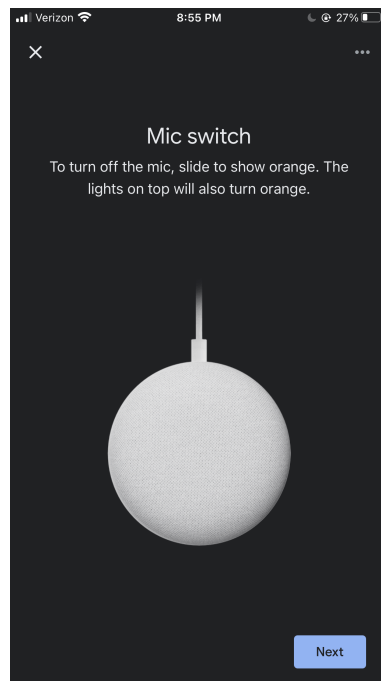
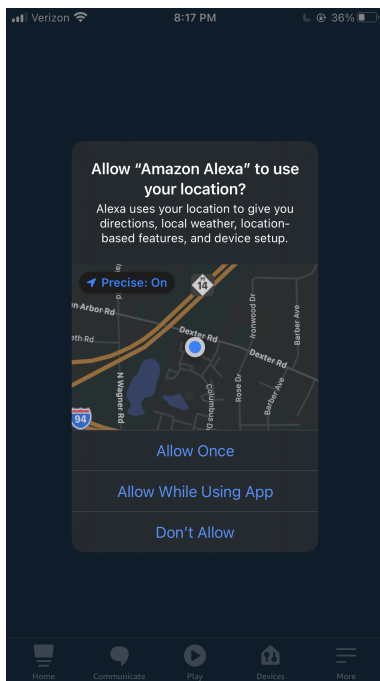


Figure 3.8: Screenshots of privacy control in the Amazon Alexa app (left) and the Google Home app (right)

My analysis concluded with the matching of the onboarding processes with the privacy notices I previously examined. Aligning these privacy notices with the onboarding process allowed me to identify if there are critical pieces of privacy information missing from this flow, and if there are areas where I believe the communication of these notices could be improved. For example, when the blue link “Learn more about your audio” on the “Saving audio is your choice” screen is clicked, the Google Home app provides a pop-up of privacy information about saving audio recordings [Figure 3.9]. I matched this screen with Google’s notice “FAQs on privacy: Google Nest,” [75] noting the section “Are my Assistant voice queries used to inform ad personalization?” [Figure 3.10]. I specifically focused on this section given what I had experienced with the nudges of third-party services and Lau et. al’s [13] findings where the non-adoption of smart speakers was due in part to users’ concerns and uncertainty about whether companies sell their personal data to third parties and how these third parties might use this data.

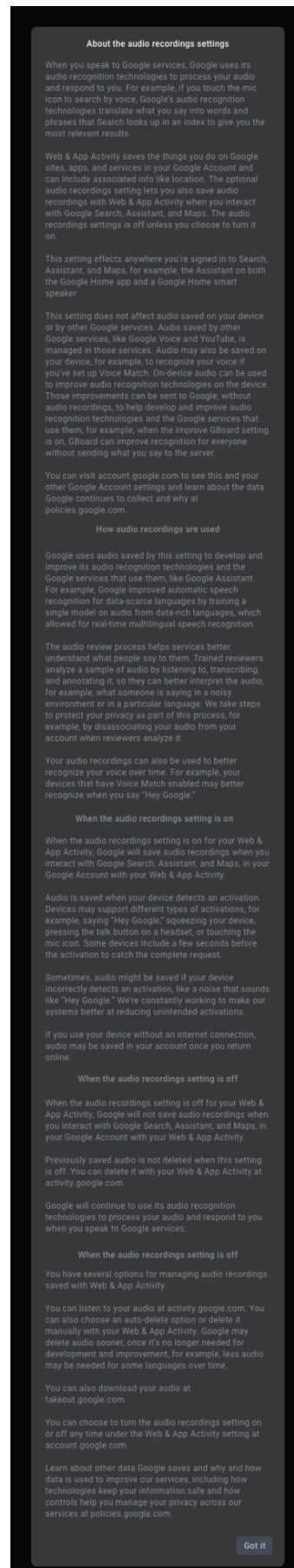
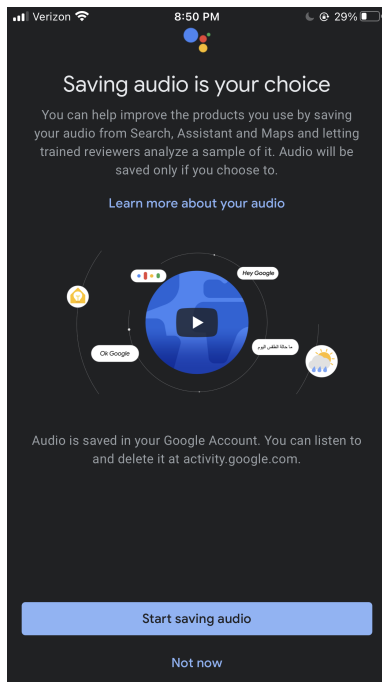


Figure 3.9: Screenshot of the Google Home app's screen regarding saving audio recordings



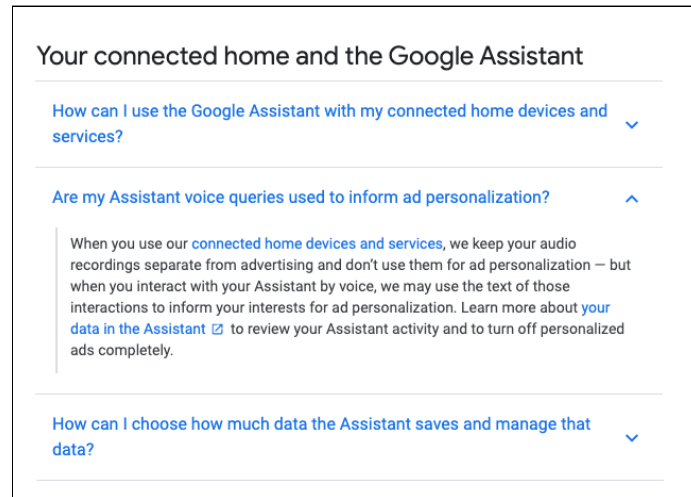


Figure 3.10: Screenshot of “Are my Assistant voice queries used to inform ad personalization?” under privacy notice for FAQs about privacy: Google Nest

The example above demonstrates how Google communicates privacy notices to their users during the onboarding process versus a general notice on Google’s website. This highlights the usability issues that previous research has found. In comparing the mobile notice versus the desktop notice, Schaub et al’s [62] findings on how limited screen estate can impede privacy notice design were underscored.

Additionally, in the Google Nest Mini’s onboarding, the privacy notice regarding saving audio recordings is exceedingly long and is difficult to read for multiple reasons. The first reason being that the text is incredibly word-heavy and is laden with jargon. In order to get a better idea of how readable this notice is, I parsed it through a Gunning Fog index calculator [76]. The Gunning Fog index generates a readability score based off of a formula of total words, total sentences, and use of complex words (words containing three or more syllables) [77]. This formula generates a level between 0 to 20, and the level represents the education level that is required to understand the text (e.g. a score of 6 is readable by 6th graders while a score of 17 or higher requires a graduate education level to fully understand) [77]. The entire notice received a score of 13.62 with a total word count of 801 words and total complex word count of 147 words. I then used the same Gunning Fog index calculator for a FAQ answer to “Are my Assistant voice queries used to inform ad personalization?” It generated a readability score of 23.08, meaning that only users with a graduate-level education would be able to comprehend this privacy information. It is clear that both privacy notices do not even come close to meeting good usability standards.

Furthermore, the color contrast is especially light between the dark grey background and the lighter grey text. This also results in low readability as well as poor overall accessibility. It is also interesting to note that within this audio recording's notice, they do not highlight the website links [Figure 3.11].

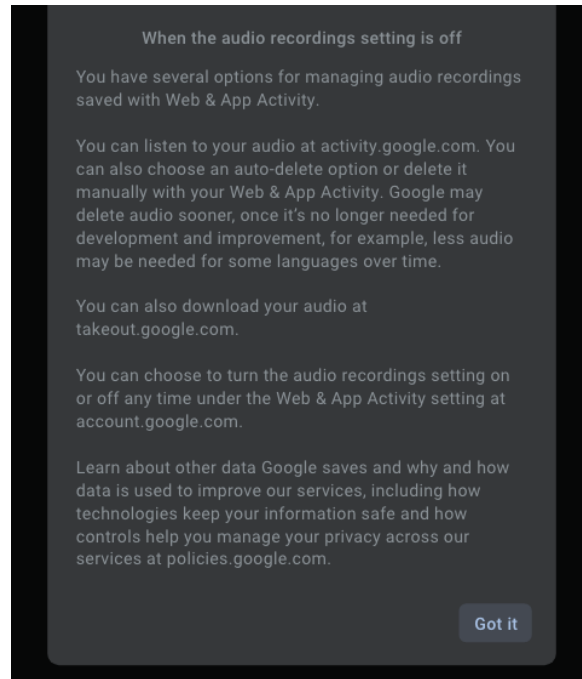


Figure 3.11:. Partial screenshot of audio recordings privacy notice in the Google Home app

Even though Google is technically informing the user of privacy choices and controls, it is not making these choices or controls prominent for the user. A user would have to take the extra step of clicking on “Learn more about your audio” and then scroll through this 800+ word document. This is significant because, as prior research has pointed out, a lack of usable and prominent privacy notices may result in user misconceptions regarding the company, their product, and their data practices [68], [69]. Moreover, a user is more likely to ignore this notice altogether if it is either not presented in a meaningful way or if it is presented at an inopportune time [65], [69]. As a result of neurological habituation, a user will most likely quickly click through it without registering any of the controls they have or risks associated with saving audio [78]. Given how long this particular notice is, combined with its jargon and a lack of prominent, informative design, this notice will most likely feel repetitive to users and consequently they will not pay attention to the privacy information that is provided.

### **3.4 Summary**

My empirical assessment of current privacy practices reinforces prior research findings in regards to privacy notice design. This analysis revealed that these practices do not meet good usability standards due to the sheer number of notices as well as their length and legalese and technical jargon [69]. They fail to be transparent in regards to how smart speakers collect, process, retain, and share users' personal information [62]. Furthermore, they do not properly highlight privacy choices and controls that users may utilize. As a result of these findings, users may be unable to provide informed consent during the smart speaker onboarding process because they do not fully understand the consequences of agreement and participant [64].

The onboarding flow analysis revealed that both the Amazon Echo Dot and Google Nest Mini employ a large number of screens for a user to navigate in order to complete onboarding. The Google Nest Mini dedicates a number of screens solely for sponsored third-party services. Both flows show that users are not provided with the ability to interact with the smart speaker devices until at least halfway through the onboarding process. Furthermore, this analysis illustrated a lack of transparent, usable privacy information in both the Amazon Echo Dot and Google Nest Mini onboarding processes.

## CHAPTER 4

### Design of a Privacy-Conscious Onboarding Flow

In this chapter, I describe designing and building a privacy-conscious smart speaker prototype. I explain my rationale for the specific design I chose and describe the challenges I faced in building a prototype that could be tested remotely due to Covid-19. I conclude this chapter with the finished smart speaker prototype including the design intervention of privacy-oriented voice commands.

#### 4.1 Design Rationale

I chose to evaluate only the Google Nest Mini and its corresponding Google Home app because of the findings from my onboarding flow analysis. In order to conduct this evaluation, I recreated the Google Nest Mini's onboarding process to help me gauge its effectiveness in helping users understand the smart speaker's functionalities. In addition to this baseline evaluation, I also wanted to test the large number of screens on users to see if they had any negative reactions to them. I was interested in capturing users' thoughts on the sponsored third-party screens due to Abdi et al's [12] research finding of users typically not considering third-parties as having access to their data. Additionally, I had noticed more UX design decisions within the Google Nest Mini and Google Home App, such as low color contrast and not highlighting links that relate to privacy control, that appeared to be deliberate, or at the very least careless, in making privacy information, choices and controls less prominent. Furthermore, Google is internationally renowned in the UX world for their Material Design [79]. Material Design is a design language created by Google and released in 2014 that mimics the physical world through pleasant-looking, rich features such as cues, motions, and lighting [80]. As a UX designer, I was curious to evaluate how these esteemed designs performed in front of users.

In addition to evaluating the Google Nest Mini's overall onboarding process, I also wanted to analyze how this process affects users' awareness of privacy awareness. My empirical assessment of the Google Nest Mini's privacy practices and its onboarding flow revealed that the onboarding process fails to provide usable privacy notices. Moreover, prior work has shown that users' misconceptions of smart speakers stem from their limited understanding of smart speakers and their related data activities, including collecting, processing, and sharing [12], [68], [81]. This contributes to a lack of awareness and understanding in how users can protect themselves while using a smart speaker [12], [55], [81]. As a result, I decided to add privacy controls as another concept to evaluate.

## 4.2 Specific Design Decisions of the Prototype

I also chose to integrate the specific privacy control of privacy-oriented voice commands, into my prototype for four reasons. The first being that, I could easily replicate the design, layout, and voice interactions since the Google Nest Mini and its Google Home app already provided example voice commands during its onboarding process.

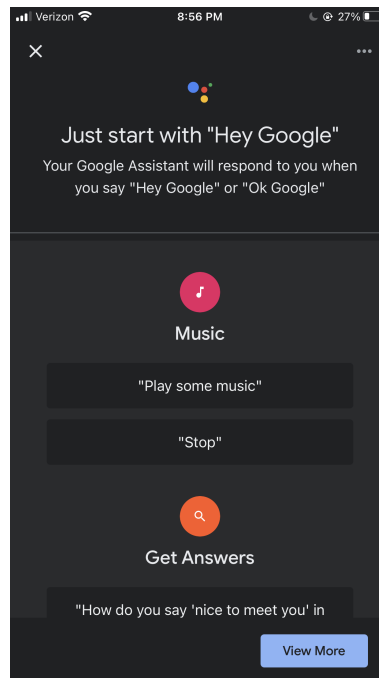


Figure 4.1: Screenshot of example voice commands in the Google Home app

Second, the Google Nest Mini now provides users with the ability to use basic commands to control their privacy such as, “Hey Google, delete what I just said” [82]. However, my analysis of its current onboarding flow found that it does not make users aware of these voice interactions. This allowed me to test a currently available privacy control to see if users react to it in any way, and build off this privacy control to provide users with greater flexibility in regards to controlling their privacy. Third, the testing of privacy-oriented voice commands within a smart speaker’s onboarding process is a novel idea. To the best of my knowledge, little to no formal, academic research has been conducted on this topic. Furthermore, prior research has shown that a mixed modal approach of voice and visuals is a way to help users understand device functionality without increasing the users’ cognitive load [58] which demonstrates that this is a promising idea. Finally, the integration of privacy-oriented voice commands worked well in regards to evaluating the effectiveness of a smart speaker’s current onboarding process. This was because these commands were a small, benign intervention, yet would still allow me to

examine the effectiveness of the overall onboarding as well as if these commands had any effect on users' awareness and understanding of privacy.

#### **4.2.1 Design Challenges as a Result of Covid-19**

I designed a prototype that modeled the Google Nest Mini smart speaker and was able to be interacted with via Zoom. Extenuating circumstances drastically altered my approach to designing my prototype and running my study. The Covid-19 pandemic introduced a number of challenges when it came to building the smart speaker prototype. In a non-Covid world, I would have been able to conduct my research in a lab setting. This would have made my designing and evaluating my prototype relatively straightforward. I would have used Adobe XD to design my prototype because it provides voice capabilities including voice commands and speech playback [83]. Even more beneficial is that Adobe XD has a specific integration with Google Assistant which allows designs to be transferred and tested on a Google Assistant device [84]. In a lab setting, I would have been able to deploy the voice technology to the Google Nest Mini and test out the mobile app onboarding on a lab-owned smartphone.

Instead, I had to figure out how I was going to get this in front of users while still creating a realistic smart speaker prototype for them to interact with. I originally began designing my prototype in Adobe XD, as it allows for prototyping voice capabilities and can easily be shared to external parties via a link. I planned on conducting an unmoderated study using Prolific--a respected, online user research platform [85]--in order to evaluate my prototype. This would have allowed me to conduct my research in a remote manner without requiring me to moderate every study as well as achieve statistically significant, quantitative results through Prolific's large participant pool. I intended to have my study participants first test the prototype and then complete a survey in Qualtrics to gauge how effective the onboarding process was, and to measure their awareness and comprehension of privacy information. During the ongoing pandemic lockdown, I realized that my study setup would not work in the way I had originally planned because participants would have to navigate between multiple platforms in order to complete my study. I was concerned that this would not only cause a large number of unfinished studies but also that the back and forth between online platforms could affect my study results.

I went back to the drawing board to see if there were other online platforms where I could run unmoderated user testing using an Adobe XD voice prototype and a survey. This proved to be extremely difficult, as most user testing platforms only have the capabilities to host a prototype with strictly click interactions and no voice commands or speech playback. Cost was also a factor I considered because many of these platforms charged up to \$500 a month to run user tests. Given how many constraints I experienced as I tried to find a way to conduct unmoderated user testing, I pivoted the design of my study to a moderated approach. This consisted of me running individual studies where I oversaw the testing of the two versions of my prototype and conducting users interviews via Zoom virtual conferencing software. While this added more onto my plate in terms of recruiting, scheduling, and running individual studies, it also afforded me greater flexibility and the opportunity to capture rich, nuanced data such as body language, probing into users' decisions, etc.

Resolving the design of my study was not the only hurdle I ran into as a result of the Covid pandemic and its pervasive effects. I also experienced many difficulties and design constraints with Adobe XD for prototyping. Since I was trying to recreate the Google Nest Mini's onboarding process, I needed to make sure that each component was as realistic and accurate as possible. For many screens, I simply used screenshots that I took during my personal user testing of the device. I would add layers onto these screenshots to make them interactive. However, many screens were dependent on prior decisions made by the user, which required an if/then functionality. Additionally, the onboarding process begins with an optional video within the app. At the time of designing my prototype, Adobe XD did not allow the use of embedded videos. I felt this was an important component that could not be left out because the opening video might provide insight into its effectiveness of the overall onboarding process. Adobe XD also did not allow for hyperlink functionality. Many app screens included hyperlinks to Google's privacy notices [Figure 4.2]. If a user were to link on one of these hyperlinks in a real world setting, they would be taken to Google's website with the linked notice via an external browser.

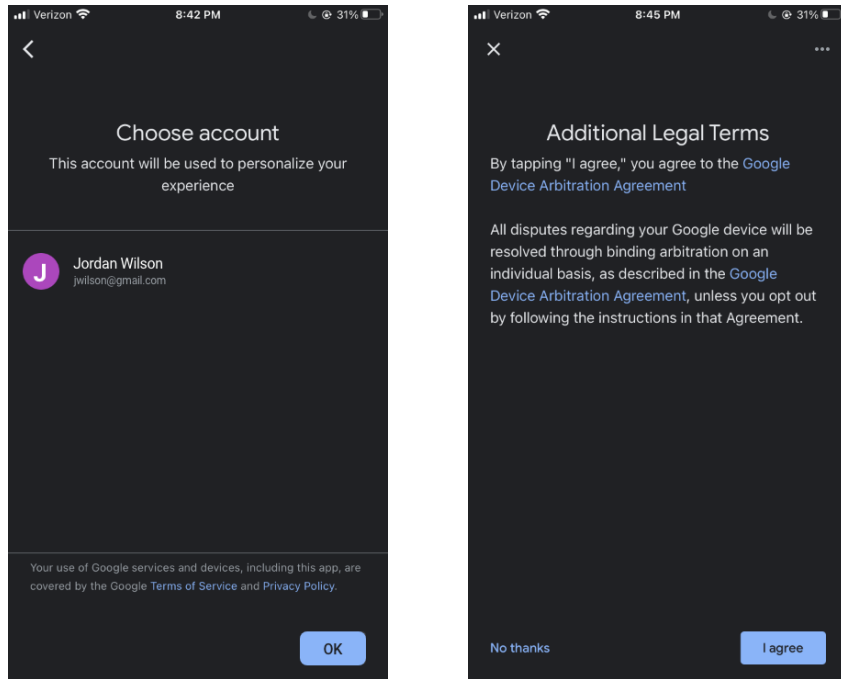


Figure 4.2: Screenshots of hyperlinks in the Google Home app's onboarding

This proved to be the most difficult design constraint and one that I could not overcome. If I wanted to continue to use Adobe XD, I would have had to assemble screenshots, piece by piece, of the mobile versions of each linked privacy notice. Furthermore, many of these notices contain additional links [Figure 4.4]. In order to reconstruct a highly accurate and realistic onboarding process, this meant that I would have to assemble dozens more of linked notices on the off chance that a user might click on them.



## Information your device may send to Google servers when you choose to share device stats and crash reports

Here's what information is sent to Google servers when you choose to share device stats and crash reports for a particular Google Nest device using the "Help improve your device" setting. This applies to [Google Nest and Google Home devices](#), [Chromecast and Chromecast Ultra devices](#), [Chromecast Audio devices](#), [Chromecast built-in devices](#) (except for Android TV devices), and [Google Assistant speakers](#). For Android TV devices with Chromecast built-in and Chromecast with Google TV devices, see the [Android Help Center](#) instead for more information on how your device stats and crash reports may be shared with Google.

Figure 4.4: Screenshot of additional hyperlinks listed under a Google privacy notice

After much research, I chose to utilize Protopie [86]. Most tools did not allow voice capabilities as well as video, hyperlink, and if/then functionalities. Protopie provided all the needed functionalities with the added bonus of an Adobe XD integration. This meant I could fine tune the details of each onboarding screen and then plug them into Protopie to program the corresponding realistic interactions.

### 4.3 Final Prototypes

In order to evaluate both the Google Nest Mini's onboarding process and privacy-oriented voice controls, I designed two versions of the same prototype [Figure 4.5]. The first version which was the control condition, closely mimicked the Google Nest Mini's current onboarding process. The second version, the treatment condition, was very similar to the control group except that a section within its example voice commands had been altered to include privacy-oriented ones. I chose these specific commands based on my analysis of the current privacy practices. I felt that smart speaker's responses to these commands would inform users of unexpected privacy practices.

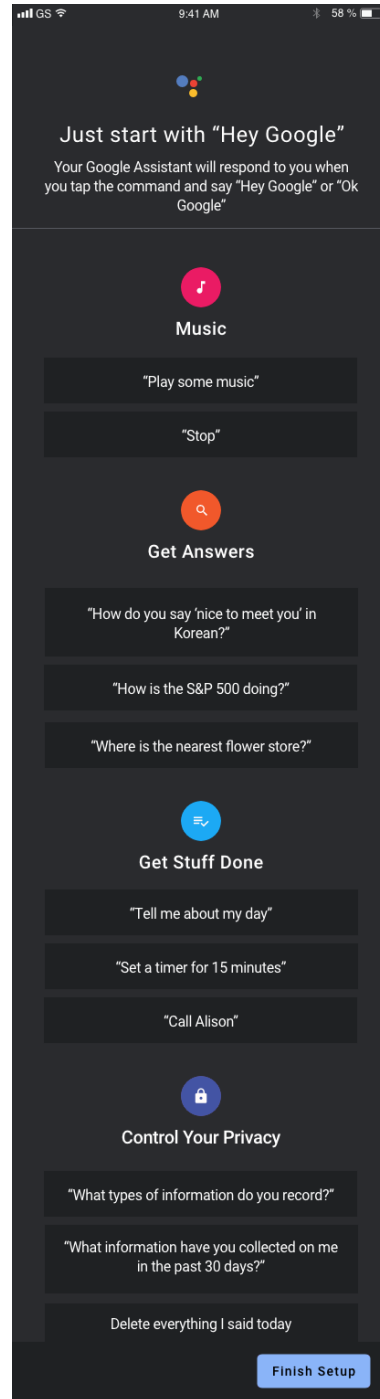
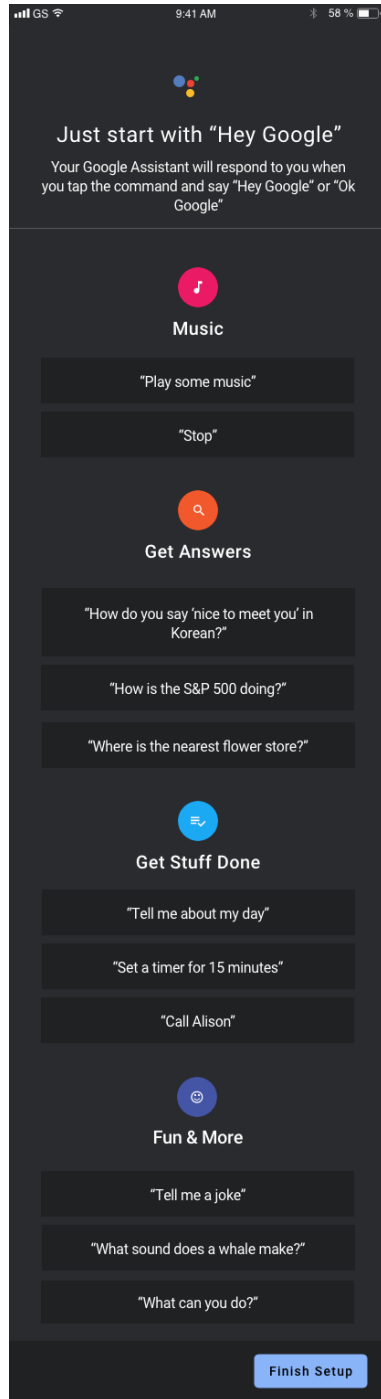


Figure 4.5: Screenshot of original example voice commands (left) and screenshot of privacy-oriented voice commands (right)

I also made the decision to cut down on the number of screens in the Google Nest Mini's onboarding process. Through pilot testing, I found that 73 screens was far too many screens for users to get through within a 60 minute testing session. Thus, I cut out screens that were similar in interaction or topic. For example, setting up Voice Match originally consisted of 5 screens and required the user to speak 4 commands [Figure 4.6]. I cut this section down to 3 screens with 2 commands [Figure 4.7].

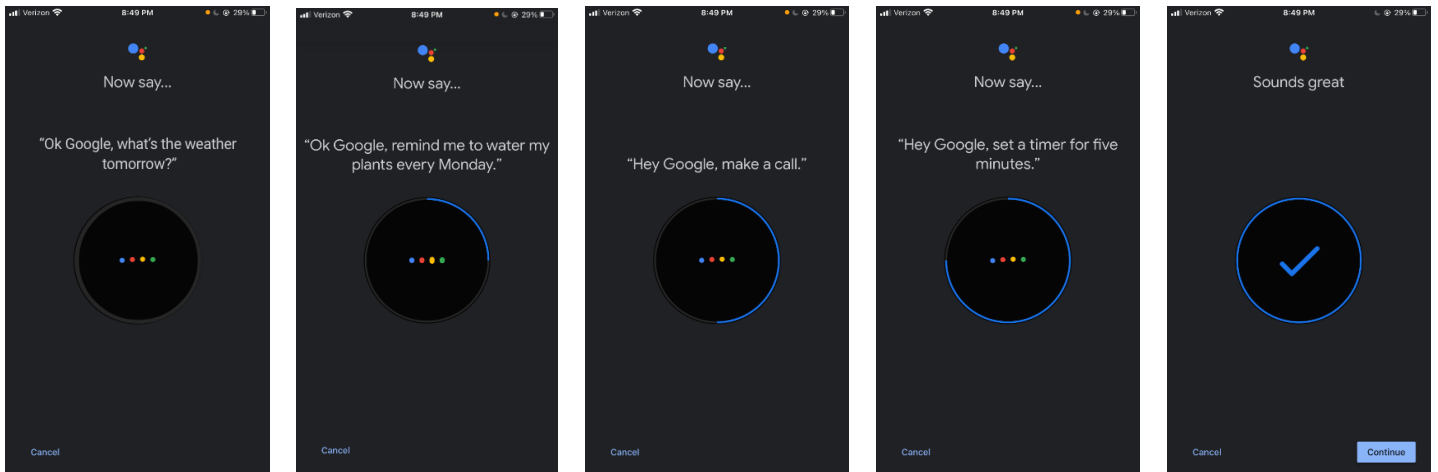


Figure 4.6: Screenshots of Voice Match setup in the Google Nest Mini's original onboarding process

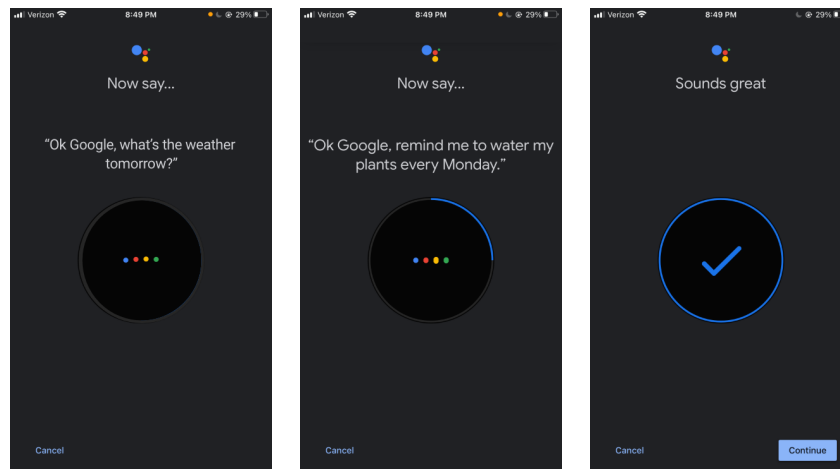


Figure 4.7: Screenshots of Voice Match setup in prototype

I also made design alterations when screens allowed for a wide variety of choices. Due to prototyping constraints, I was unable to exactly mimic these screens. Similar to my approach with cutting down the number of onboarding screens, I simply cut down the number of choices [Figure 4.8]. It is important to note that none of these altered screens and their narrowed down choices involved privacy information or privacy controls.

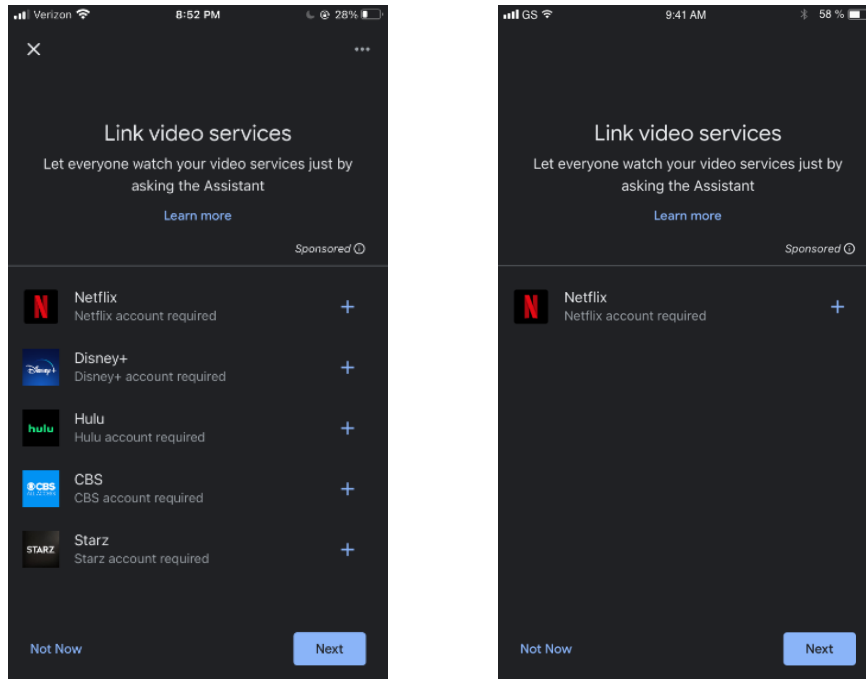


Figure 4.8: Screenshots of the original “Link video service:s screen (left) and the modified version of “Link video service”s in the prototype (right)

The final design alteration I made to these onboarding screens was the use of motion-based imagery. Since I took screenshots, I did not capture these motion images nor was I able to find these exact images in an available, downloadable file. Given that Google’s Material Design is known for its pleasing use of motion in its design [80], I felt this was an important aspect to replicate. As such, I simply replaced these with images from LottieFiles [87] that I felt closely resembled the originals [Figure 4.9].

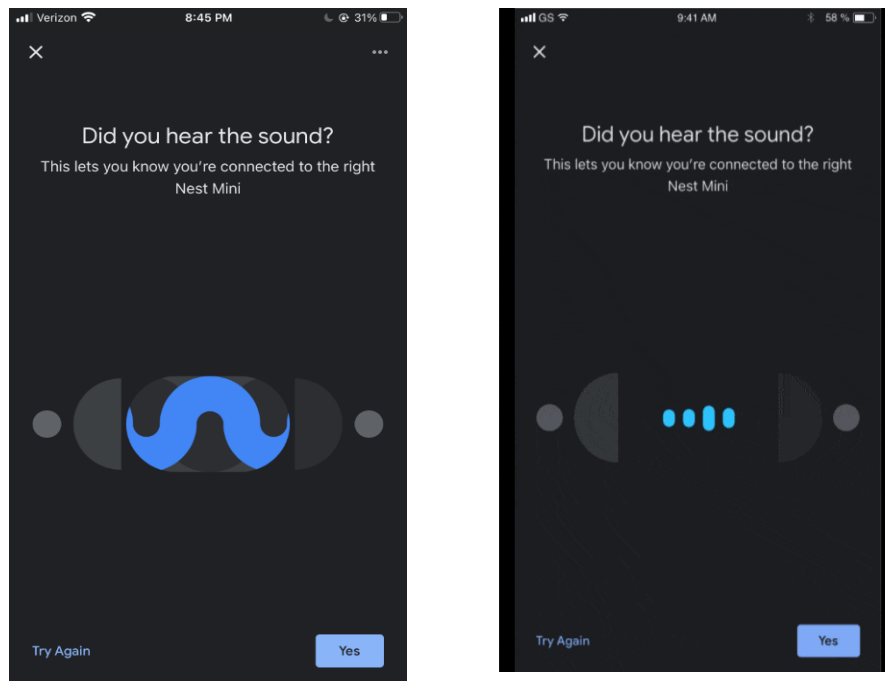


Figure 4.9: Screenshots of the original “Did you hear the sound?” screen (left) and the modified version of “Did you hear the sound?” in the prototype (right). Please note, the image on the right is a screenshot so it does not fully demonstrate the movement of the inserted Lottie image.

#### 4.4 Demonstration & Explanation of Final Prototype with Privacy-Oriented Voice Commands

I provide a written demonstration of my smart speaker prototype with the added privacy-oriented voice commands below [Figure 4.10]. This shows how the smart speaker responds to the user’s privacy voice commands. I also provide an explanation for why I chose each privacy-oriented voice command.

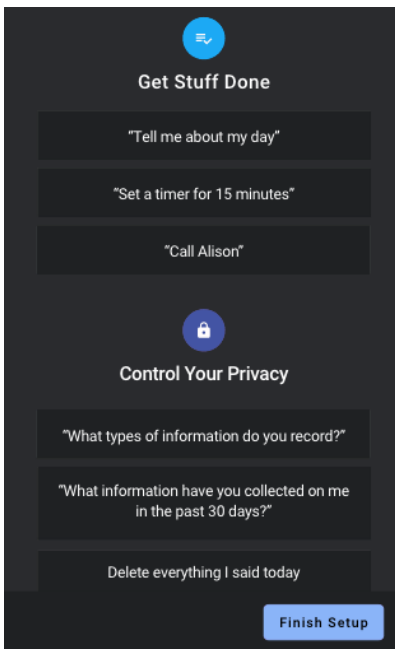


Figure 4.10: Screenshot of privacy-oriented voice commands

When a user says, “Ok/Hey Google, what types of information do you record?” the prototype responds with, “I might record different categories of personal information such as your name, phone number, and location, demographics including your age, gender, and language, as well as other types of personal information. To learn more, check out the Google Nest Privacy Help Center.” I chose this specific command due to my analysis of current privacy practices that was discussed in Chapter 3. My online research found that many people did not fully understand the specific types of information collected by smart speakers, and that they might find some of these practices to be quite unexpected. The reason why I had the prototype end its response with “...to learn more, check out the Google Nest Privacy Help Center.” is because that is how many of the Google Nest Mini’s current privacy notices conclude. They encourage users to check out the Help Center or some other privacy-related notice that is found online. I was curious to see if users in my study would react differently because being audibly encouraged to check this out rather than having it be communicated in a visual notice. Lastly, I wanted to consider Google as a company and whether they would actually employ a command such as this. To make a better business case for privacy-oriented voice commands, I used similar response language from the Google Nest Mini for other non-privacy voice commands whether the speaker encourages the user to learn more by checking out Google’s website.

When a user says, “*Ok/Hey Google, what information have you collected on me in the past 30 days?*” the prototype responds with, “*You’ve found a privacy routine. You can set up a monthly summary about what types of information have been collected on you. Let’s try it together. First, the following information has been collected: the music you listened to, your location, the search terms you asked me, and the contact information that is connected in your phone book. Do you want me to remind me of this privacy routine in 30 days?*” The user can either say “*Ok/Hey Google, yes.*” or “*Ok/Hey Google, no.*” If the former, then the prototype will say, “*Okay. In 30 days, I will provide you with another summary about what information has been collected. And just so you know, you can say delete everything I’ve said today or customize more privacy controls at myactivity.google.com.*” If the latter then it responds with, “*Got it. And just so you know, you can customize your privacy controls at myactivity.google.com.*” I chose this second command because I was inspired by my previous research, specifically of Luger and Rodden’s [55] argument that informed consent should attempt to reengage and reconnect with users over time rather than a single notification.

I also wanted to test out a layered privacy notice that drew inspiration from Schaub & Cranor [69]. They explain this approach as, “Notices and controls can be layered. A short notice may highlight a practice, fact or control to gain the user’s attention and provide a link to additional information or more controls, which in turn might consist of multiple layers that users can reveal and explore as needed. In UX design, this design pattern is called details on demand—providing an overview or summary first, with options for users to retrieve details. Thus, rather than trying to provide a single notice or control that does everything, it’s better to craft a privacy UX that is composed of many complementary privacy notices and controls at different levels of detail tailored to the respective user group and context. A privacy UX combines privacy interfaces shown at different times, using different modalities and channels, and varying in terms of content and granularity in a structured approach. With such an integrated and multilayered approach, individual users still receive information and choices for data practices that pertain to them but won’t be confronted with data practices that are irrelevant for them until they are using a respective feature of the system. Users should still have the option to read the full privacy policy and explore all privacy settings whenever they want” [69]. With this privacy command, a user receives a layered notice that is relevant to the specific privacy practice they are inquiring about without receiving a lot of excess information. Additionally, the speaker will attempt to reengage with them over time to remind them of this privacy practice rather than utilizing a single notification. Finally, similar to the first privacy-oriented voice command, this one also makes a business case for Google. It utilizes a routine which is a Google Nest Mini-specific feature and encourages the user to check out more information through Google’s website.

When a user says, “*Ok/Hey Google, delete everything I said today.*” the prototype responds with, “*Okay. I deleted all the system activity from midnight to just now. You’ll be able to see the change in your system activity page in just a moment.*” I chose this third and final privacy-oriented voice command because of Lau et al.’s [13] recommendation for future research concerning voice commands that encourage users to delete their recordings. Additionally, this is already a voice command that is allowed by the Google Nest Mini. Yet through my analysis of current onboarding flows, I found that it is not a command that is made apparent to users. Given this, I found it especially important to make this specific command salient and provide the exact response that the speaker currently provides in a real world setting.



## CHAPTER 5

### Online Evaluation Study

#### 5.1 Online Evaluation of a Smart Speaker's Onboarding

In this chapter, I present the analysis and results from the online evaluation of the Google Nest Mini's original onboarding process and the onboarding process with privacy-oriented voice commands. The goal of this online study was threefold: to evaluate how users navigate through the onboarding process, how the onboarding process affects their awareness of controls to protect their privacy, and whether privacy-oriented voice commands help users feel more in control of their personal data.

##### 5.1.1 Method

I conducted an online usability test followed by a cognitive interview with 13 participants via Zoom conferencing software. This was a between-subjects study with a control group and a treatment group. The control group tested the Google Nest Mini prototype that mimics the original onboarding process, and the treatment group tested the prototype with privacy-oriented voice commands. Participants were instructed to “think aloud” as they went through and interacted with the prototype. The goals for the usability test were to identify elements of the onboarding process that specifically help users learn the smart speaker's functionalities, and to test if the privacy-oriented commands have an effect on users' awareness of privacy. The goals for the cognitive interview were to test if participants in the treatment group had a better understanding of privacy information as a result of the privacy-oriented voice commands, and if participants in either group had similar perceptions or misconceptions as previously discussed in the related work section. I measured these goals using participants' think-aloud feedback during the usability testing (e.g. what they found surprising, what they had trouble with, etc.), and their responses from the cognitive interviews. The usability test and cognitive interview techniques allowed participants to provide insights regarding how useful they found the onboarding process and example voice commands to be as well as any difficulties they encountered. I used these insights to uncover patterns and themes which then allowed me to assess participants' comprehension of the Google Nest Mini and its privacy controls, as well as pinpoint the areas where the speaker's onboarding process could be improved. The study was exempted by the University of Michigan Institutional Review Board. Below I discuss the recruitment, study procedure, results of the qualitative analysis and limitations of this work.

### 5.1.2 Session protocol / instruments

Those interested in participating in the study first filled out a screening survey to determine if they currently or have previously owned a smart speaker. Interested participants who answered no to this question received an invitation to sign up for an online usability test and cognitive interview session. They also had the option to fill out additional questions probing into why they do not own one as well as their demographics [Appendix C]. I targeted those who do not own a smart speaker in order to prevent potential biases that could result from people who had previous experience with setting up a smart speaker device. Moreover, people who do not own a smart speaker may be more privacy concerned than those who do, which might make them more resigned when making privacy decisions than those who do [88]. This would allow me to test Lau et. al's [13] recommendation of "designing privacy information with resigned users in mind."

Each session was conducted via Zoom. Participants were assigned to either the control or treatment group based on age, gender, and their rationale for not owning a smart speaker as noted in the screening survey. Participants were divided into two groups: control and treatment. The control group of participants tested the prototype with the control condition (no privacy-oriented voice commands), and the treatment group of participants tested the prototype with the treatment condition (contains privacy-oriented voice commands). During the session, participants were given a prompt, and were instructed on how to physically interact with the prototype [Appendix D]. They were also instructed to think aloud on each screen in the onboarding process. I then shared my screen with the participant and gave them remote control access over the mouse so that they could interact with the prototype on their own. Due to conducting this study remotely, the prototype was a combination of the Google Nest Mini smart speaker and its corresponding app. Thus, instead of the participant being onboarded through the app and speaking to the smart speaker device, this would all be done within the app itself.

I tracked the interactions and choices made by each participant throughout the onboarding process using a spreadsheet [Appendix E] which contained a list of all possible interactions a participant could make on each screen. This allowed me to quickly record all aspects of the usability test which made analyzing my results much more efficient because I did not need to go back to every single recording to remind myself of participants' click paths. The cognitive interview had two phases to it. The first phase involved asking participants to express their thoughts, feelings, and decision rationale concerning the prototype and onboarding process' content and design. To test the effectiveness of the onboarding process itself, participants were asked what aspects they found to be most helpful and most confusing. The second phase consisted of asking participants about specific screens concerning privacy and notices. To aid in their memory recollection, I again shared my screen with the participant and

displayed the specific screen about which I was inquiring. To evaluate how effective the onboarding process is regarding privacy awareness and controls, participants were asked questions aimed at measuring their comprehension of how the Google Nest Mini collects and uses their information [Appendix F]. Specifically, they were asked what privacy controls are available to them to protect their privacy from the smart speaker and how they would go about using these controls and changing their privacy settings.

### **5.1.3 Recruitment & Participant demographics**

Participant recruitment consisted of posting invitations on social media channels including Twitter, Facebook, LinkedIn, and spreading it through word of mouth. Participants were compensated \$15 for taking part in the online evaluation study. I recruited 13 participants for the online evaluation study. Participant demographics are listed in Table 5.1.

ID	Assigned Group	Gender	Age Range	Race/Ethnicity	Education	Primary Occupation
P1	Control	W	25-34	Hispanic, Latino/a/x, or Spanish	Bachelor's degree	Business, Management or Financial
P3	Control	M	35-44	Hispanic, Latino/a/x, or Spanish	Master's degree	Business, Management or Financial
P7	Control	M	25-34	White	Bachelor's degree	Student (Graduate, Doctoral)
P8	Control	W	35-44	White	Bachelor's degree	Service
P9	Control	W	25-34	Asian	Bachelor's degree	Business, Management or Financial
P11	Control	W	25-34	White	Bachelor's degree	Administrative Support
P2	Treatment	W	18-24	Asian	High school	Student (Undergraduate)
P4	Treatment	W	25-34	White	Master's degree	Education or Science
P5	Treatment	W	25-34	Asian	Master's degree	Student (Graduate, Doctoral)
P6	Treatment	W	55-65	White	Bachelor's degree	Business, Management or Financial
P10	Treatment	M	25-34	White	Master's degree	Business, Management or Financial
P12	Treatment	W	35-44	White	Master's degree	Business, Management or Financial
P13	Treatment	W	25-34	Black or African American	Master's degree	Education or Science

Table 5.1: Participant Demographics of Online Evaluation Study

#### 5.1.4 Analysis Approach

The usability test and cognitive interview sessions were audio and screen recorded to capture all feedback from the participants. Transcription services were enabled during Zoom. Once the session was complete, I downloaded these transcripts into separate Google docs, one per participant. Any identifying information that was found in these transcripts was either replaced (e.g. replacing participants' names with their participant ID) or deleted. No other information was changed. A thematic analysis [89] of the transcripts and the participant interaction spreadsheet was conducted to identify overarching themes, patterns, and issues.

### 5.1.5 Limitations

This study has several limitations related to the prototype design and the sample size.

While Protopie did solve many constraints, I still had to concede to some design limitations.

I made the decision to integrate the smart speaker functionalities into the Google Home app rather than the original direct interactions with the smart speaker since much of the onboarding does not require the user to physically interact with the Google Nest Mini device. It would also be impossible for a participant in this study to physically interact with the device because it was run remotely via Zoom. This meant that instead of talking to a physical smart speaker, a user would instead speak to the app which would then respond in the same manner as the Google Nest Mini. This became a limitation because users expected more system feedback than they received. It was difficult for them to tell when the Google Nest Mini prototype was listening because it did not light up in the way that the actual device does.

Additionally, in order for the app to know when and how to respond to voice commands, a trigger would need to be employed by the user. This took the form of a click or tap by the user. Normally, a user would just need to say “Hey Google” or “Okay Google” and the speaker would activate. Yet my prototype needed a physical trigger, such as the user tapping a specific area of the app with their mouse, in order for the speaker to begin listening and then activate the proper response. This proved to be a limitation of the prototyping tool because it created an additional step for participants to remember while interacting with the speaker. Another limitation of the tool was that I was unable to provide as much flexibility and choice options as the original onboarding app (discussed in Chapter 4). This might have resulted in participants paying less attention to certain screens or elements, or they might have behaved differently with the prototype than they would have with the real app.

While 13 participants is a respectable number for cognitive interviews [90], this study would benefit from a greater sample size to further test the effectiveness of the Google Nest Mini’s onboarding process and the effect privacy-oriented voice commands have. Additionally, about half of the participants noted in the screening survey that they have privacy concerns with smart speakers. This could limit the results because these participants may be more privacy-oriented than the standard smart speaker user.

## 5.2 Results of the Online Evaluation Study

In this section, I present the results of the prototype's usability test and cognitive interviews. In the results, I combined participants from both the control and treatment groups because only 1 participant (P6) interacted with the privacy-voice commands. P6 practiced, "*Delete everything I said today.*" The response to this command does not provide additional privacy information but only confirms that action has been taken. Therefore, participants in the treatment group did not receive privacy information that could have influenced their responses during the cognitive interviews. I only discuss the separate groups in the results section regarding privacy-oriented commands. Participants found the onboarding process to be fairly simple and straightforward but felt they did not receive enough useful information to understand the Google Nest Mini's full functionalities. Additionally, participants found privacy-related screens to be some of the least helpful parts of the onboarding process. While the results of the study found my design intervention of privacy-oriented voice commands to be ineffective, these types of commands do show potential for future research.

### 5.2.1. Perceptions of the Onboarding Process

Overall, most participants felt the onboarding process to be straightforward. 9 participants said it felt familiar and standard--especially in comparison to other onboarding processes they've experienced. P11 mentioned, "*I felt like it was easy. It felt very similar to probably any other kind of onboarding process or task that has been set up.*"

#### Ease of Use With the Google Home App's User Interface

The Next buttons were a common theme, as 6 participants mentioned them when recalling their overall onboarding experience. Participants had expressed that these buttons provided them with directionality while navigating through the onboarding screens. P12 noted, "*I think, overall, it was really quite simple. It was very linear like I felt like I knew what to do. Every single page told you what to do next. I would say, most of the time, almost every single time I knew where to click, what to click, the icon geography was helpful, and there were little buttons down in the corner that asked me to move on.*"

Additionally, 4 participants specifically mentioned the Next button when asked about what they found to be the most helpful part of the entire flow. P10 recalled, "*I don't know if there was anything that was overly helpful, other than it kind of prompts you when you're ready to go to the next step. I don't think there were many, if any situations where I sat there wondering, 'Wait what am I supposed to do?' Is something next or am I ready to go to the next step? It's very seamless in that way.*" These buttons helped participants quickly navigate the onboarding in order to finish setting up the Google Nest Mini. Participants also used these buttons as an escape route. 10 participants used them as a way to move on

from confusing information or when they were unsure of what was required from them. P6 said, “*I think there was maybe one thing that I wasn't exactly sure what to do, but I also know you can't really break anything so you just keep clicking around until you figure it out.*” P5 described a few screens as, “*It was like a bunch of words and there was an option to go next, so I just went next.*”

### **Vague Information and Terminology**

The majority of participants were surprised by the amount of text shown during the onboarding process. While only 2 participants specifically noted how much reading was required when asked what the least helpful or most confusing part of the onboarding process was, all participants had mentioned large amounts of text during their testing of the prototype. Many of them noted that they found this text difficult to understand due to vague terminology of the speaker's functionalities such as “Personal results. When presented with the personal results screen during onboarding [Figure 5.1], P8 commented, “*The term personal results is somewhat confusing. Like it I don't understand what that means. But I assume I have to agree to that.*”

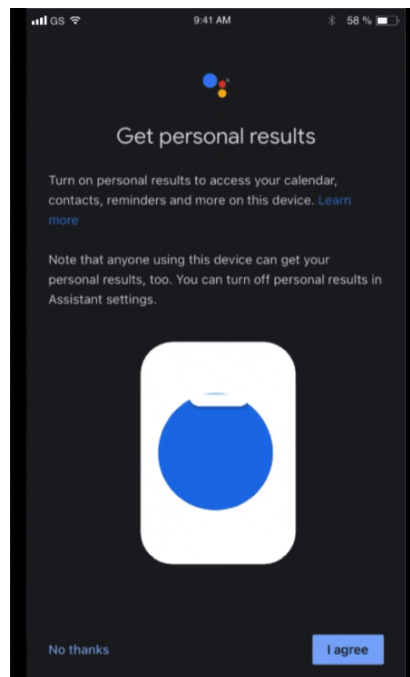


Figure 5.1: Screenshot of Personal Results screen

Some participants even had trouble deciphering differences between the Google Home app, the Google Assistant, and the Google Nest Mini speaker. When presented with the screen in Figure 5.2, P4 said “I’m not sure what a Google Nest Mini is, but we’re going to find out.” P2 explained, “As someone who doesn’t have experience with the Google Home, I don’t know if it’s referring to stuff in my home, the devices, or the Google Nest Mini device itself.” When describing their experience with the onboarding, P11 said, “I suppose I thought that the onboarding was going to be voice. I thought the onboarding was going to happen via interacting with the speaker itself, so I thought that was going to be pretty cool. So the fact that it was an app and that the app was called Home, it just felt incongruent with what we were actually doing...I just thought I was setting up a voice speaker with Google Assistant that’s all I thought I was doing.” When asked during the cognitive interview if they were confused by prototype setup or if their confusion was caused by something else, P11 clarified that they felt they were not properly informed during the onboarding process that the speaker’s mobile app was called something other than Google Nest Mini. P11 explained that they knew about the voice assistant being called “Google Assistant” because they own an Android phone.

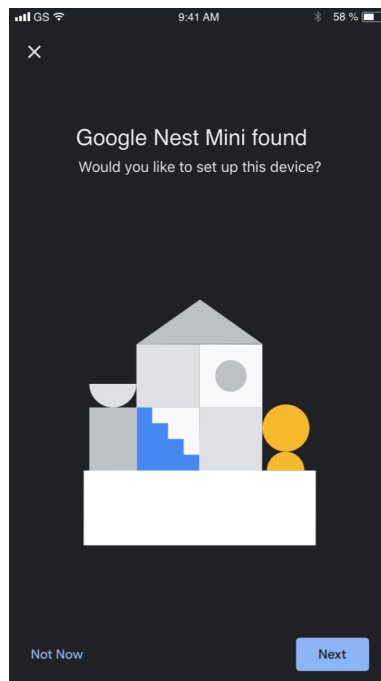


Figure 5.2: Screenshot of Google Home app connecting to Google Nest Mini smart speaker



## Understanding of the Google Nest Mini's Functionalities

Most participants felt they did not receive enough instructional information as to how the Google Nest Mini functions. 5 participants mentioned that they would want to separately search for answers to their questions about the speaker's capabilities while 3 said they are still confused as to how the speaker works with other connected devices and/or services. The majority of participants were especially confused by Google Duo [Figure 5.3], as this was a service they had never heard of before. Moreover, they did not understand how calling the smart speaker with a voice command actually worked or how guests in their home could interact with it. P9 said the onboarding process did not address understanding the linkage between the Google Nest Mini, the app, and other connected devices, *"I guess that just kind of still blurry in my mind like how do they all sync?"* P5, P6, P8 and P10 all mentioned that they would look up the functionalities of the speaker online in order to specifically learn how it reacts to users who have not set up voice match with the device. When asked if there was anything else they wanted to mention about their experience with the onboarding, P8 mentioned that they were still confused about Voice Match. *"I would wonder if I have to go and find other family members and set them up, or if it's just going to listen to whoever talks to it?"*

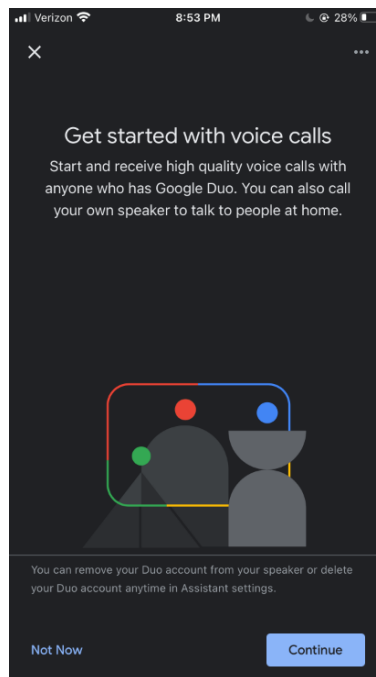


Figure 5.3: Screenshot of Google Duo service

### Specific Privacy Notices & Interfaces

During the onboarding, 7 participants clicked on one or more of the drop-down carets when they encountered the Set Up Google Assistant [Figure 5.4] screen. Only P13 clicked on the Learn More link under Services and Your Privacy. They expressed resigned frustration when they said, *"I'm confused... but I guess Google system is different than the Nest so that was..this is a little confusing...So, it doesn't look like there's any way to not do this so kind of just feels..I don't know..."* Only 2 participants, P2 and P13, clicked on the links located on the Additional Legal Terms screen [Figure 5.5]. P2 said, *"Okay with these smart homes, I would want to read the legal terms, but let's see how long it is before I decide if I'm going to read it thoroughly [clicks on arbitration link]. Oh it's not that long, I guess, I should actually read this in case... [skims through it] Okay, I was expecting to read stuff about my rights to privacy, but I don't really see anything about that so i'm just gonna exit out. Okay, I guess, this isn't about my privacy rights. It's more about like I agree not to sue Google. Okay, I guess, I agree."* P13 again expressed frustration but this was due to the fact that they were taken out of the app and to an external browser where the Arbitration agreement was linked.

Yet 13 participants specifically noted the "privacy screens" when responding to questions about their experience with the Google Nest Mini during the cognitive interview. 4 participants remarked that they found these screens to be the most confusing part of the onboarding. When prompted to clarify which specific screens they were referring to, all participants identified Set up Google Assistant, and about half of the participants identified the Google Arbitration Agreement and Voice Match [Figure 5.6] as well.

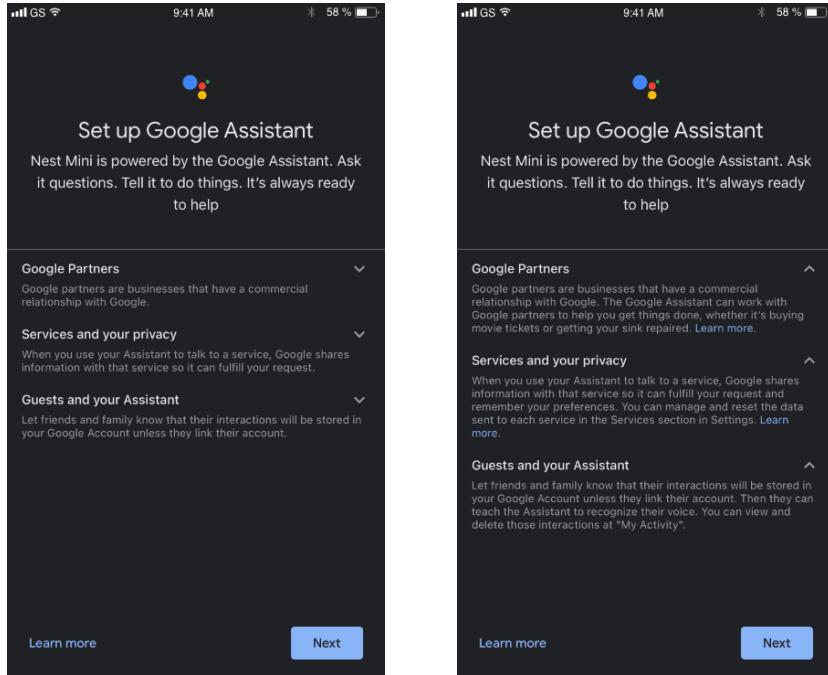


Figure 5.4: Screenshots of collapsed and expanded versions of Set up Google Assistant screen

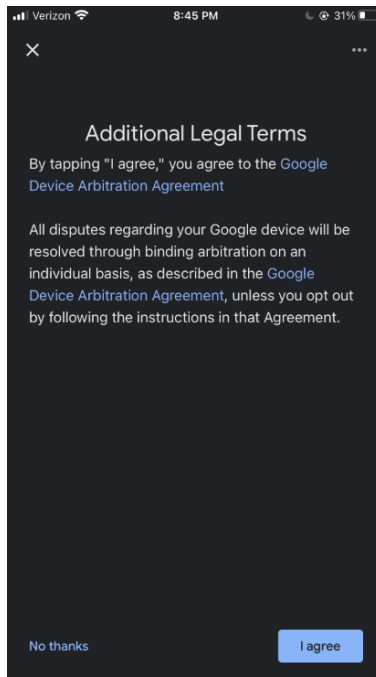


Figure 5.5: Screenshot of Google Arbitration agreement screen

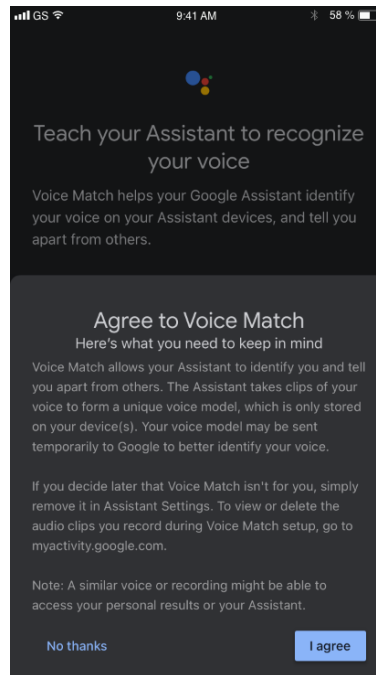


Figure 5.6: Screenshot of Voice Match agreement screen

Participants had mixed feelings regarding the Set up Your Google Assistant screen. 7 participants clicked on the individual drop-down carets to expand the selection. Only 1 of these participants clicked on the Learn More link. P4 said that they felt like they had to read through this entire screen but it *“made it clear that you’re in control of what data is being collected.”* P11 said that this screen *“made the whole process easy to go through”* in regards to agreeing to Google’s privacy policy. However, this illustrates a clear disconnect. P11 along with 5 other participants referred to this screen as Google’s privacy policy, the terms of service, or the terms & agreements. This screen is not any of these things and there is no consent or agreement is required from the user. None of the participants even clicked on the actual privacy policy or terms of service links within the onboarding. When asked why and if they noticed these links, half of the participants said they saw the links but did not feel the need to click on it because they know those links are full of jargon and long text. This relates to the previously discussed prior research on usable privacy notice design [62], [65], [69], [78].

Participants also mentioned the number of agreements they encountered during the onboarding process. 3 participants found these agreements to be a type of red flag. P5 recalled, *“It was a little annoying that there were so many things that you had to agree to, because I’m one of those people, I don’t actually read them but at the same time, that makes me nervous, seeing that there’s so many of them. So afterwards I’d probably want to google or ask around how people are thinking about what the machine is actually doing.”* This demonstrated another disconnect between the onboarding process and the

privacy screens, specifically the Voice Match screen. Participants were asked what types of information is collected by the Google Nest Mini, when and what does the Google Nest Mini do with this information, and who has access to this information? 7 participants said the Google Nest Mini collects everything and 11 participants said it collects information all the time. Both of these are incorrect. Only 3 participants correctly said that the Google Nest Mini can only collect their information when they speak directly to it using the trigger word. Furthermore, 5 participants incorrectly said the Google Nest Mini sells their information and 5 said it's used for some type of marketing and targeted ads. What may be most interesting is that no participants listed themselves as having access to this data. Part of this could be due to the fact that this was preceded by other privacy-related questions. But given that the onboarding process promotes that saving audio is the users choice and they can listen to their audio and delete it through their Google account, this demonstrates that users may still not feel in control of their personal data. The answers to the questions are found within the Voice Match and Set up Your Google Assistant notices yet it is apparent through participant responses that these notices are not usable enough to prevent these information disconnects and misconceptions.

Lastly, 6 participants mentioned the design of these privacy screens. All 6 said they felt easy to click through and agree (similar to the Next button findings), and 3 of these participants commented that they appreciated the formatting of the various text headings which helped them skim (e.g. Google Partners, Services and Your Privacy, etc.). However, the other 3 participants who mentioned the screen design said they felt like the content of these screens was too difficult to skim through and that their appearance made them feel less important. P12 elaborated, *“But I feel that it intentionally is not attention grabbing. Like it's really gray, it's hard to read, you got a nice little blue button down at the bottom that's urging you to keep going. It doesn't require you to read it, you know, so those are the things I think about.”* P2 echoed a similar sentiment, *“Honestly...the interface of it just doesn't draw me in, and I feel like with something as important as your privacy Google should do something to make it a little bit more like flashy flashy or something like that. It just feels unethical in a way that Google decides to put the most important thing, towards the end and doesn't even like make a bigger deal of it than how it really is like this just looks like such a basic page anyone would skip”*

## Privacy Control Needs

When asked what the current controls are to protect one's privacy from the Google Nest Mini, 8 respondents mentioned the opt-in and agreement screens they encountered during the onboarding process. 6 participants brought up the mute button they previously interacted with. This demonstrates that the onboarding process could be a useful way to inform users of privacy controls because the participants were able to quickly recall these screens and identify them as privacy controls. However, 2 participants who mentioned the mute button said that they do not trust it and 3 other participants remarked that they are still suspicious that these controls do as they promise. P3 explained, "*Well the engineer, he says it's probably like a digital button but it's not exactly like a power on off button because the power stays on. So, is it really muting or is it muting the device and still listening, or is it muting? Everything about it was unclear.*" This illustrates the need for having users practice using these controls to facilitate trust between the user and the device.

When asked if the privacy controls and settings of the Google Home Mini were sufficient, participants had mixed responses. 5 participants said no, 4 responded that they wanted more control options, 3 said they were unsure, and 4 said yes. Participants who responded no did so because they found that the controls either defeated the purpose of owning the speaker, or found the controls too shrouded by process. P1 explained, "*I think the purpose of it is you being able to be on the other side of the room and say 'Hey Google' and requesting it to do something. So if I had to turn it on and off every time I wanted it to listen to a command then I'd have to be within the vicinity of the Google Home any which kind of defeats the purpose, because I might as well, if I had to walk somewhere and then walk to the Google Nest Mini, I might as well just walk to the light switch and turn it on it off.*"

It is interesting to note that the majority of yes responses were not because participants felt like the controls were usable but rather that they felt that they met the necessary legal requirements. P7 reasoned, "*You know there's no way to really get away from your information being collected. But like I said they're doing as much as they are legally required to. And that's about all we can really hope for, I think in 2021.*" Participants who said they wanted more controls clarified that it wasn't necessarily that they wanted different control options but rather that they wanted more transparency about these options. P3 said, "*If there were more privacy controls like up front and center about it and they were more transparent about those things, then yeah, I would like that more...that would be really helpful for me to say 'Okay well, they're proactively worried about what I want [to control] about myself rather than what they would like.'*"

It is also interesting to note that the participants who said they were unsure responded this way because they were unaware of the controls they could use to protect themselves. All three participants said that they did not know because they did not read through the fine print information. P6 said, *"I didn't read all those tiny words...yeah the legalese stuff it's painful."*

In summary, participants found the onboarding process to be fairly straightforward as a result of salient cues such as the Next button. Vague terminology caused confusion for participants especially in regards to how the Google Nest Mini recognizes users' voices and syncs with other products and services. Additionally, participants found screens with privacy-related information to be perplexing. Participants did understand that opt-in and agreement choices were a form of privacy controls during the onboarding, yet they expressed needing an extra layer of reassurance that these controls deliver what they promise.

### **5.2.3 Interventions With the Onboarding Design**

The intervention with the privacy-oriented voice commands [Figure 5.7] was not effective during the usability test. Three of the seven participants in the treatment group noticed them, and only one participant practiced with a single privacy command, "Delete everything I said today." When asked about their thoughts on this, P6 said, *"I like that Control Your Privacy thing, but it would be nice...oh I guess it doesn't say...I would want to see what information have you collected on me in the past 30 days actually on the computer screen because it could talk for 60 days to tell me was collected."* P6 did not want to try this command out but instead preferred to finish setting up. Only P4 said that they would not want to speak to the Google Nest Mini about changing privacy controls. They equated these voice commands with calling a customer service line where they just want to press zero in order to speak to a representative to get their needs taken care of.

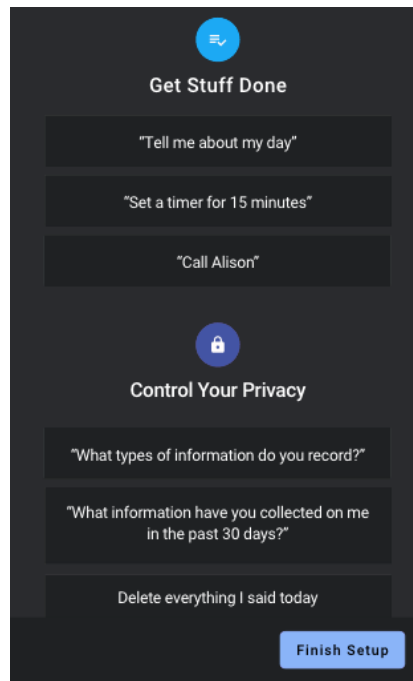


Figure 5.7: Screenshot of privacy-oriented voice commands intervention

However, findings from the cognitive interview suggest that this is a design that could be iterated upon. During the first phase of the cognitive interview, participants in both groups were asked how they felt about the voice commands. Those in the treatment group were not specifically asked about the privacy-oriented voice commands. This was to test whether participants in the treatment group mentioned them of their own accord. No participants in the treatment group brought them up in response to this question. However, I then showed the screen with privacy-oriented voice commands during the second phase of the cognitive interview, regardless of the control and treatment groups. Again, I did not point out the privacy-oriented commands but instead let participants examine the screen on their own. Of the 13 participants, 10 said that they would find them useful, with the majority saying that they did not know you could use commands such as these. These 10 participants were split evenly down the middle with 5 having been in the control group (P4, P7, P8, P9, P11) and 5 in the treatment group (P5, P6, P10, P12, P13). P7 said, *“It would be a first that I had seen or heard of. You know the speaker telling you what is actually recording is a kind of interesting concept.”* Similar to P6, two other participants said they would prefer a visual modality to receive this response. P11 suggested an audio-visual modality, *“I would rather the output be on my phone with the little Google saying something like ‘Check your phone we just sent you everything.’”*



## Privacy Command Explorations & Implications

After seeing these privacy voice commands, participants became curious what other privacy-oriented commands were possible. P10 mused, *“Delete everything I said today, so it gives you an option right now to delete it. And I wonder if there’s an option to just not allow it to or to automatically delete it?”* P3 took this a step further by expressing their desire for an in-the-moment style privacy voice command, *“I would rather ask ‘Don’t record everything I say right now.’ Maybe I would ask that, to see what the device says. If it says it can or cannot do that and to find out what the consequences are of that to like performance.”* P1 also wondered about the implications of these types of commands. They questioned if saying “delete my entire history” was similar to clearing their web browsing cookies, and whether this would mean that they would have to relink specific services to the Google Nest Mini. P5 questioned if the delete voice command actually means complete eradication of that information. They said, *“I feel like there’s still some record out there, like, even if I tell someone to delete something kinda like with Gmail. If I send something to the trash it’s still in the trash right, like I can still retrieve it. So I don’t know what ‘delete everything I said today’ means. Does it mean I won’t be able to retrieve it tomorrow, like if I said ‘delete my to do list’ but does that mean Google still has access to that to do list somewhere else?”* While the smart speaker’s response tells the user that this deletion is reflected in their Google account, it is clear that users need some form of confirmation that this command is effective.

## Placement of the Design Intervention

5 participants noted how these privacy commands are below the fold and less likely to be noticed, especially when it’s the final screen of the onboarding process. Two participants suggested having a separate screen for the privacy-specific commands because they seem to be more complex than the others. P12 explained, *“[This is] something that’s like completely different and way more complex and not something that I would think about. For this sort of setting if that makes sense, like the first three are like really simple examples that I think are pretty common that like it tested out and then there’s this other like someone like informative fourth section that feels like much more complex and a different level of things that I think would actually be better to be on a separate screen.”*

Despite the privacy voice commands current placement, the majority of participants appreciated the transparency and awareness these commands attempted to provide. P8 described them as, *“It seems more accessible. It feels like they’re being more upfront about what I can do to control my privacy and I don’t have to go digging around on the device or a website or something to try to find these controls.”*

### **Timing of voice commands**

When asked why they mentioned that the list of example voice commands was rather long and they did not feel that these types of commands applied to them at that moment. Users also described their impatience with wanting to complete the onboarding process.

In summary, the intervention of the privacy-oriented voice commands was found to be ineffective due to participants' lack of need for interacting with them. However, when further prompted, participants' reactions and responses to them make a case for further refinement and research.

## CHAPTER 6

### Conclusion

#### 4.1 Discussion

In this section, I discuss the overall results from this thesis. First, I discuss my research questions in relation to the main findings from my research including related work, the analysis of current onboarding processes and how they pertain to my research questions. I conclude my research by providing contributions to this field in the form of implications of privacy-oriented voice commands and design recommendations for the overall onboarding experience.

##### 4.1.1 Main Findings

I began my research by asking the following research questions:

1. How effective is a smart speaker's onboarding experience in meeting users' expectations and helping them understand device functionalities?
2. How does this experience influence end-user comprehension of privacy notices and controls to facilitate trust between the device and the user?

The review of related literature revealed that the onboarding process is crucial for smart speakers because it instructs users on how to interact with the device and makes them aware of the devices functionalities and capabilities [28], [34], [35], [39]. If the onboarding process is not instructional or engaging enough then it could lead to inaccurate mental models of the smart speaker's ecosystem and its privacy practices, understanding gaps in the speaker's functionalities, and could potentially dissuade users from trusting the device [12], [38], [40], [46], [48]. My analysis of current privacy practices and onboarding processes of both the Google Nest Mini and Amazon Echo Dot reinforced prior research that privacy notices typically do not engage with users in a meaningful way due to their length and complex jargon [62], [65], [69]. Moreover, current onboarding flows fail to provide privacy practices and their corresponding notices in a way that users understand and engage in.

### **UI elements met user expectations for a straightforward onboarding experience**

The findings from my online evaluation showed the Google Nest Mini's onboarding process is effective in meeting user expectations simply because its user interface provided them with the necessary guidance to move forward through the set up and onboarding. Elements such as the Next button and familiar iconography made it quick and easy for them to progress, which helped them feel like the overall process was straightforward and expected.

### **Not enough instructional information to meet user expectations for device capabilities and functionalities**

The onboarding process was not effective in helping users understand device functionalities because it did not supply them with the instructional information they needed to have an accurate understanding of the device's full functionalities. The majority of users were left wondering about how certain capabilities actually work--such as the smart speaker making calls using Google Duo--and how the Google Nest Mini syncs with connected services such as Netflix. Moreover, confusing naming conventions between the Google Home app, Google Nest Mini smart speaker device, and the Google Assistant voice assistant left users feeling unsure about how the three work together in conjunction. Some users noted that they prefer to get the onboarding process done and over with as quickly as possible so that they can begin interacting with the speaker and use it for the purposes for which it was originally purchased. However, this reliance on trial and error led them to skip necessary information that was needed for a more accurate mental model of both the device's operational capabilities but also its privacy notices as well. This reflects prior research on how trial and error can lead to understanding gaps in users [40], [46], [48].

### **Privacy notices within the Google Nest Mini's onboarding process met users' low expectations and did little to facilitate trust between the user and the device**

The Google Nest Mini's onboarding process did little to facilitate trust between users and the device. Users found privacy screens to be some of the most confusing and least helpful parts of the onboarding experience. As a result, these notices failed to connect with users in any meaningful way [65]. They outright ignored any links that hinted at being a privacy notice. Moreover, the privacy notices that they did encounter only reinforced their expectations of typical privacy notices, which resulted in them quickly clicking through the notice in order to avoid dealing with lots of text and jargon. This highlights prior research on neurological habitation with privacy notices [78]. In instances where the privacy notice was not long, such as the Set up Google Assistant screen, users were still left feeling confused and unsatisfied due to vague terminology. Some equated this screen to a terms and conditions or privacy policy agreement, despite not being prompted to agree. Users did note that the use of headings and short chunks of text on this screen helped them to easily skim the information but upon

further prompting during the cognitive interview, they said that this information was not meaningful or useful because it was not specific enough in communicating its privacy practices. This demonstrates that well-formatted privacy information can improve readability yet the information itself must be specific and concise.

### **Privacy controls show promise when made salient during the onboarding process**

The majority of users could recall specific privacy controls that they could utilize to protect their privacy from the Google Nest Mini. In addition to the physical controls such as the mute button, they also identified various opt-in or agreement choices they encountered during the onboarding process. This is extremely important because it demonstrates that users are able to identify a variety of control modalities that they can employ in order for the smart speaker to better meet their privacy preferences. Furthermore, they became aware of these privacy controls during the onboarding process, which illustrates that onboarding may be a prime channel through which to communicate these controls.

### **Users need specific instructions and reassurance regarding privacy controls**

Even though users were able to identify specific privacy controls they were still hesitant about their functionalities. Users specifically did not trust the mute button, which reinforced findings from Lau et. al [13] regarding lack of trust in smart speaker controls. Moreover, users said that they wanted more transparency regarding their available options to control their privacy. The majority of users said that they assume that controls and settings to adjust their privacy are found within the Google Home app but that they cannot be sure of this. This demonstrates that it is not enough to simply bring awareness to the privacy controls themselves. Rather, the onboarding should also provide instructions on how to access them. More importantly, it should demonstrate that these controls are reliable and actually do what they say they do. Not only would this help to facilitate trust between the user and the smart speaker, but it would also meet the previously discussed Fair Information Practice Principles [66] as a result of its openness and transparency.

### **Privacy-oriented voice commands show potential**

Finally, the intervention of privacy-oriented voice commands show potential for further research. While the intervention itself was successful, the majority of users thought these commands to be novel and useful. Users had noted that these types of commands were not something they had previously thought of even though commands such as “*Delete what I just said*” are enabled by current smart speaker devices. This indicates that the onboarding process is indeed a major opportunity for which to insert more usable privacy information to increase privacy awareness. Additionally, this bolsters prior research that discoverability is a challenge with smart speakers, especially for those devices that do not have a graphical interface [10], [28]. If users do not encounter clear affordances to help them discover

and learn about these types of privacy controls, then they are extremely unlikely to understand the functionality of these types of controls, let alone invoke or utilize them [10], [28]. Furthermore, the timing of these affordances matters. Users in both the control and treatment groups did not feel the need to practice with the example voice commands due to their impatience and them feeling like none of these commands were applicable at that moment. Since these commands were simply optional examples with which to practice, users skipped over them. Therefore, the timing of privacy controls should be considered when inserting them into the onboarding process.

## **4.2 Implications of Privacy-Oriented Voice Commands**

In this section, I consider various implications of privacy-oriented voice commands and how they might be refined for future research and use.

As previously discussed, users' enthusiasm towards privacy-oriented voice commands shows promising potential for further design iterations and research. As such, the implications of these types of privacy controls should be considered. Even though the commands are audio in nature, users would prefer a mixed-modality response from the smart speaker. Users noted that they did not want the speaker to rattle off all information that has been collected on them as this would not only be extremely lengthy but would also be difficult to follow. This requires careful consideration regarding the design of the visual modality including skimmability, familiar but specific language, and reinforcements that these controls are indeed trustworthy.

Participants also mentioned their interest in other types of privacy-oriented voice commands after seeing the example privacy commands. Suggested commands included asking the smart speaker about its privacy notices, or to tell the speaker that it is not allowed to record anything the user says. Therefore, the smart speaker should be prepared to answer a variety of questions concerning both the user's individual privacy preferences as well as explain its privacy practices in layman's terms. Similar to the visual design, this will also require careful considerations in terms of the audio modality.

## **4.3 Design Recommendations for the Smart Speaker Onboarding Process**

In this section, I provide a set of design recommendations for the smart speaker onboarding process. While these recommendations are aimed at speakers without graphical interfaces, they are still applicable to many other styles of smart speakers and onboarding processes for smart devices in general because they employ good usability standards [62], [69].

First, the onboarding process should clearly indicate what actions are required by the user. This can be done through the use of graphical elements within the user interface, such as clearly-labeled buttons and brief sections of instructional text positioned at the top so that the user quickly notices them. If a screen or section of the onboarding process is optional, it should be labeled as such. When using text, it should be broken up into small sections with each section labeled by a clear header. This will improve skimmability and readability. Furthermore, the onboarding process should signal when the entire process is complete and not just when the device is set up. Users may confuse a complete device set up as being finished with learning how to interact with it. To assist users in obtaining an accurate understanding of core device functionalities and capabilities, the onboarding process should either provide relatable use case examples or require the user to practice with these functionalities. This will allow the user to understand how to properly utilize these functions, and could help prevent users from relying on trial and error. Finally, privacy notices within the onboarding process should be both noticeable and transparent. They should not hide behind a hyperlink, nor should their visual design blend in or require endless scrolling by the user. These notices should succinctly state privacy information that can be comprehended by both novice and advanced users alike. This privacy information should employ specific language to highlight its data collection practices--including what data is being collected, who has access to this data, what this data is used for, and how long the data will be stored. Most importantly, these privacy notices should include specific instructions that put control into the users' hands. Similar to the notices, these instructions should contain specific, actionable language that users can easily recall even after the onboarding process is complete.

#### **4.4 Summary**

While HAL 9000 from 2001: A Space Odyssey is fictional, in many ways he is becoming much more real due to the pervasive use of smart speakers and their rate of innovation. Given the widespread adoption, especially during the Covid-19 pandemic, special attention should be paid to ensure users are aware of a device's privacy and data practices, and the control options they can employ to protect their privacy. In this thesis, I developed a smart speaker prototype to identify where its onboarding process is effective at helping users understand the speaker's functionalities and capabilities. I tested the novel intervention of privacy-oriented voice commands within the onboarding process to determine if this type of affordance facilitates trust between the user and the device. Taken together, the results suggest that there is a strong potential to use the onboarding process as a way to inform smart speaker users of privacy information and privacy controls.

## APPENDICES



## APPENDIX A

### Coding Framework Template for Privacy Practices

Question	Answer to Question	Quote	Section	Location
<b>What data is being collected?</b>	Biometric, health, location	"We may collect location, health, ...."	Privacy Policy	Paragraph 1
<b>How is the collected data being used by the company?</b>				
<b>Who else is the company sharing the data with?</b>				
What privacy measure are put in place to protect users?				
What types of controls do users have?				
What types of risks and/or consequences are communicated to users?				

[Coding framework spreadsheet for the Google Nest Mini and Amazon Echo Dot privacy practices linked here](#)

## APPENDIX B

### Onboarding flows of the Amazon Echo Dot and Google Nest Mini

[Onboarding flows for the Google Nest Mini and Amazon Echo Dot linked here](#)

## Appendix C

### Screening Survey

**Questions marked with an asterisk are required \***

Instructions: Thank you for your interest! In order to move forward, please complete the following consent form and brief survey. You will be contacted by email if you are selected to participate in this study.

#### **Consent form**

##### **Title of the Study**

Qualitative evaluation of a smart speaker's onboarding processes

##### **Investigators**

Gina Herakovic (Master's Student, University of Michigan)

Florian Schaub, Ph.D. (Assistant Professor, University of Michigan)

##### **Study Purpose**

We hope to learn how effective smart speakers' onboarding processes are in helping users understand how they work and how to interact with them.

##### **Procedures for the Study**

If you agree to participate in this study (U-M study ID: HUM00195204), you will be asked to participate in one video-recorded usability testing session lasting anywhere from 45 to 60 minutes. The usability test involves interacting with a series of mobile screens that walk you through the onboarding of setting up and interacting with a smart speaker (a type of speaker with a voice-activated virtual assistant). We are not able to provide you with all details about the study at the beginning of the study, but we will provide more information directly after your participation in the study. The usability test will occur at a mutually agreed upon date and time, and will take place via a web-conferencing system called Zoom. It is up to you to choose the date and time to participate in the study. At the end of the user testing, we will ask you to complete an interview where you verbally answer questions asked by the moderator.

##### **Risks and Benefits**

There are minimal risks to you, most of which concern identifying you as a participant. See the "confidentiality" section below for how the team will address these risks.

You are not expected to personally benefit from participating in this research. However, others may benefit from the knowledge gained from this study. Different individuals have different understandings of smart speakers and the ways in which they interact with them. This study will help us better understand how effective the onboarding process is when setting up a smart

speaker. This study will also help us provide more comprehensive recommendations for companies who produce smart speakers and similar smart devices.

### **Financial Information**

For your time and full participation in this study you will receive \$15 that will be delivered electronically.

### **Confidentiality**

The research team will protect your privacy. Your name, contact information, and any other identifiable information will be stored separately from the study data and will only be used for scheduling purposes and payment processing. The research team will further remove any identifying information from the study data, including recordings and transcripts, before analysis. This study data will only be accessible to the research team and will be stored in U-M computing services certified for human subjects use. Quotes and snippets of recordings may be used in publications and presentations of this work but no identifying information will be revealed in these materials.

The usability test and corresponding interview will be recorded and transcribed for analysis purposes. The transcription may be aided by the use of an automated external service. Audio files will be manually edited to remove names, or any other identifiable details, prior to being uploaded to any such service.

The research team will retain recordings for 3 years in order to verify and validate the accuracy of the reported findings. The research team cannot guarantee absolute confidentiality. Your personal information may be disclosed if required by law. Minus these exceptions, the research team will not allow access to identifiable data.

### **Contacts for Questions or Problems**

For questions about the study, contact the principal investigator, Gina Herakovic ([umichthesistest@umich.edu](mailto:umichthesistest@umich.edu)).

As part of their review, the University of Michigan Institutional Review Board Health Sciences and Behavioral Sciences has determined that this study (HUM00195204) is no more than minimal risk and exempt from on-going IRB oversight.

### **Voluntary Nature of Study**

Taking part in this study is voluntary. You may at any time opt-out of answering questions and/or stop your participation completely. You may also request to have your data destroyed if you elect to leave the study. Leaving the study will not result in any penalty or loss of benefits to which you are entitled. Your decision whether or not to participate in this study will not affect your current or future relations with the University of Michigan.

### **Your Consent to Participate in the Research Study**

By clicking the Next/Agree button, you are agreeing to be in this study. Make sure you understand what the study is about before you click this button. If you have any questions about the study, you can contact the study team using the information in the section above.

*I understand what the study is about and my questions so far have been answered. I agree to take part in this study.*

[Next/Agree button]

### **Screener Survey**

- Are you currently over the age of 18? \*
  - Yes
  - No
    - i. If NO they are screened out
      - 1. “Thank you for your interest in our research! Your participation has not been selected for this study at this time.”
- Do you currently own or in the past have you owned a smart speaker (a type of speaker with a voice-activated virtual assistant) device such as an Amazon Echo or Google Home? \*
  - If YES:
    - i. If YES they are screened out
      - 1. “Thank you for your interest in our research! You do not qualify for further participation in this study at this time. However, we are still interested in learning about your use of smart speaker(s). If you are inclined, we would appreciate you answering the following optional questions.”
        - a. Which smart speaker(s) do you have? Check all that apply:
          - i. Amazon Echo
          - ii. Google Home
          - iii. Google Nest
          - iv. Facebook Portal
          - v. Other - fill in the blank
        - b. How did you obtain your smart speaker(s)?
          - i. I purchased it
          - ii. I received it as a gift
          - iii. I received it as a part of a promotion while purchasing a different item
          - iv. I won it as a prize
          - v. Other - fill in the blank
        - c. How long have you owned your smart speaker?
          - i. Less than 1 month (30 days)

- ii. 1-3 months
- iii. 4-6 months
- 7 months - 1 year
- iv. More than 1 year
- d. How often do you use your smart speaker(s)?
  - i. Every day
  - ii. Once a week
  - iii. A few times per week
  - iv. Once a month
  - v. A few times per month
  - vi. A few times per year
  - vii. Almost never
- e. How many smart speakers do you own?
  - i. 1
  - ii. 2
  - iii. 3
  - iv. More than 3
- f. [Optional Demographic questions added here- see questions below]

○ If NO:

1. Have you considered purchasing a smart speaker for use in your home? \*

a. If YES:

- i. Why did you decide not to purchase a smart speaker for your home? Select all that apply: \*
  - 1. It costs too much
  - 2. It's too limited in what it can do
  - 3. The smart speaker would always be listening
  - 4. Someone could hack into the smart speaker and spy on my home
  - 5. The smart speaker company would have too much access to my personal information
  - 6. The smart speaker company could share my personal information with third parties
  - 7. Other - fill in the blank

b. If NO:

- i. Why haven't you considered purchasing a smart speaker?
  - 1. It costs too much
  - 2. It's too limited in what it can do
  - 3. The smart speaker would always be listening

4. Someone could hack into the smart speaker and spy on my home
  5. The smart speaker company would have too much access to my personal information
  6. The smart speaker company could share my personal information with third parties
  7. Other - fill in the blank
2. [Optional Demographic questions added here- see questions below]

### Demographic Questions

- What is your age?
  - a. 18-24
  - b. 25-34
  - c. 35-44
  - d. 45-54
  - e. 55-64
  - f. 65+
- What is your gender?
  - a. Man
  - b. Woman
  - c. Non-binary
  - d. Prefer not to disclose
  - e. Prefer to self-describe
    - i. [if the last option is checked a free form field opens up]
- What is the highest level of education that you have completed?
  - a. High school
  - b. Vocational/technical school (2 years)
  - c. Some college
  - d. Bachelor's degree
  - e. Master's degree
  - f. Doctoral degree
  - g. Professional degree (MD, JD, etc.)
- Which of the following best describes your primary occupation?
  - a. Administrative Support (e.g. secretary assistant)
  - b. Art, Writing, or Journalism (e.g. author, reporter, sculptor)
  - c. Business, Management or Financial (e.g. manager, accountant, banker)
  - d. Education or Science (e.g. teacher, professor, scientist)
  - e. Engineering or IT Professional (e.g. programmer, IT consultant)
  - f. Homemaker
  - g. Legal (e.g. lawyer, law consultant, or law professor)
  - h. Medical (e.g. doctor, nurse, dentist)
  - i. Service (e.g. retail clerk, server)

- j. Skilled Labor (e.g. electrician, plumber, carpenter)
- k. Unemployed
- l. Retired
- m. Student (Undergraduate)
- n. Student (Graduate, Doctoral)
- o. Other - fill in the blank
- Select all you identify as:
  - a. Hispanic, Latino/a/x, or Spanish
  - b. Native American Indian or Alaska Native
  - c. Asian
  - d. Black or African American
  - e. Native Hawaiian or Other Pacific Islander
  - f. White
  - g. Unknown
  - h. Prefer to self-describe - fill in the blank
  - i. Prefer not to say
- What is your email address?\* This will be used to contact you if you are selected for participation in the study. Your contact information will be protected and will only be used for scheduling purposes.
  - a. Fill in the blank

“Thank you for taking the time to complete this survey! You will be contacted by our research team shortly if you are selected to participate in the study. If you have any questions or concerns please contact the principal investigator, Gina Herakovic ([umichthesistest@umich.edu](mailto:umichthesistest@umich.edu)) Thank you again!”



# Appendix D

## Usability Test Script

### Introduction and Instructions to Usability Test

Hello [Name],

Thank you for your willingness to participate in this study. I am [introduce self] and I am a graduate student at the U of M's School of Information. I am working with Dr. Florian Schaub to study how effective the smart speaker onboarding process is for users in helping them understand how they work and how to interact with them. In the case that either my or your internet goes out, I will reach out through email and reschedule our session.

I will now start the recording and enable transcription [begin recording on Zoom and enable transcription].

How this study will proceed is that I will share my screen with you and I will give you remote control access over the mouse. There might be a slight lag in the mouse at first after I transfer control to you. I will also turn my camera off so that it feels like you are by yourself with your phone. You will be shown a series of mobile phone app screens. You can interact with these screens as if they were an app on your phone. Some screens will ask you to talk to a smart speaker. In those instances, tap on the screen with your mouse and speak clearly into your laptop's microphone in order to have the smart speaker respond to you. Does this make sense?

As you make your way through the screens, please say what you are thinking out loud. This might feel a bit uncomfortable or awkward, but this helps us understand everything you are experiencing during the onboarding process. For example, "I am going to click on this button that says 'Next' because I think it will get me to the next page." You are allowed to ask questions while interacting with the prototype but understand that I may not be able to answer them depending on what you have asked.

Following this task, you will be asked about different aspects of your experience. Please answer these questions openly and honestly. There are no right or wrong answers. We value your honest thoughts. Are you ready to begin with the study? As a reminder, please remember to say everything you are thinking out loud.

[Moderator shares prototype screen with participant and gives them remote mouse control access]

Imagine your name is Jordan Wilson and you live in Ann Arbor, Michigan. You have purchased a Google Nest Mini smart speaker for your home [hold up Google Nest Mini to show participant what it looks like]. You have just unboxed the speaker and plugged it in. Now you are following

the onboarding process through the Google Home app on your mobile phone in order to set up your Google Nest Mini.

[Turn off camera]

This ends the first task. This page isn't clickable but feel free to look at and tell me your thoughts. Thank you for completing this task. I will now ask you about your experiences with this task. This is the final part of this session. Similar to the task, I want you to say everything you are thinking out loud. These questions are designed to help us test the effectiveness of the prototype, not you or your abilities. Are you ready to begin?

[After participant is done, stop sharing screen]

[Begin reading cognitive interview questions]

### **Debrief Script**

*If Control Group (no voice command privacy controls):*

This usability test and interview is now complete. Thank you so much for taking the time to test our prototype and for answering our questions. Now that the session is over, we can provide you with the full details of this study. In addition to looking at the overall effectiveness of a smart speaker's onboarding process, we are also examining if it influences a person's perceptions and awareness of their privacy. The prototype you tested closely mimics Google Nest Mini and its onboarding process. Other participants have interacted with a prototype whose example voice commands have been altered by the research team. Do you have any questions or concerns about this?

I will now need to collect your mailing address so that you can receive your compensation for participating in this study. This information will be submitted to the Human Subject Incentives Program at the University of Michigan. Only myself and HSIP will have access to your mailing address and once the check is processed and mailed, this information will be deleted. What is the best mailing address to use for you to receive your check? [Write down mailing address] Delivery time has been varying between a few business days to a couple of weeks depending on the Post Office. Be on the lookout for an envelope with a return label of "University of Michigan Shared Services Center A/P." Do you have any questions about your compensation?

Thank you again for your time. This has been extremely valuable for our research.

[Stop recording]

*If Treatment Group (has voice command privacy controls):*

This usability test and interview is now complete. Thank you so much for taking the time to test our prototype and for answering our questions. Now that the session is over, we can provide you with the full details of this study. In addition to looking at the overall effectiveness of a smart speaker's onboarding process, we are also examining if it influences a person's perceptions and awareness of their privacy. The prototype you tested mimics the Google Nest Mini and its onboarding process. However, the example voice commands you were given have been altered. The example voice commands about privacy are an added design by the research team. Other participants have interacted with a prototype that closely mimics the Google Nest Mini with no design alterations. Do you have any questions or concerns about this?

I will now need to collect your mailing address so that you can receive your compensation for participating in this study. This information will be submitted to the Human Subject Incentives Program at the University of Michigan. Only myself and HSIP will have access to your mailing address and once the check is processed and mailed, this information will be deleted. What is the best mailing address to use for you to receive your check? [Write down mailing address] Delivery time has been varying between a few business days to a couple of weeks depending on the Post Office. Be on the lookout for an envelope with a return label of "University of Michigan Shared Services Center A/P." Do you have any questions about your compensation?

Thank you again for your time. This has been extremely valuable for our research.

[Stop recording]

## Appendix E

### User Interaction Decision Tree Spreadsheet

Due to its size, the user interaction decision tree spreadsheet is unable to be displayed within this appendix. [The User interaction decision tree spreadsheet linked here and is available for public viewing here.](#)

## Appendix F

### Cognitive Interview Questions

1. Tell me about your experience with the Google Nest Mini's onboarding process?
  - a. What, if anything, did you find most helpful?
    - i. Why?
  - b. What, if anything, did you find confusing or least helpful?
    - i. Why?
2. [If participant used practice voice commands]
  - a. Tell me how it felt to practice voice commands with the Google Nest Mini?
3. What, if any, types of information do you think the Google Nest Mini collects?
4. What do you think the Google Nest Mini does with what you say?
5. When do you think the Google Nest Mini can collect this type of information?
6. Who do you think has access to this type of information?
  - a. Why do you think that?
7. Do you feel like the Google Nest Mini provided clear information on its data collection practices?
  - a. Why/Why not?
8. What controls, if any, are available for you to protect your privacy from the Google Nest Mini?
9. How would you go about changing the privacy settings on the Google Nest Mini?
10. Would you consider these controls and settings sufficient?
11. Ask about specific screens/interactions here:
  - a. [Clicked on Terms of Service or Google Privacy Policy]:
    - i. Why did you click on this link?
  - b. [Did not turn on Bluetooth/Local Network/Location Access after downloading the app]:
    - i. Why did you not not allow this setting?
  - c. [Share device stats/crashage reports with Google Agreement]:
    - i. Why did/didn't you choose to/not share these reports with Google?
  - d. [Voice Match Agreement]:
    - i. Why did/didn't you choose to use Voice Match?
  - e. [Skipped controls on speaker]:
    - i. Why did you skip the screens on the Google Nest Mini's controls?
  - f. [Voice commands]:
    - i. Did you notice you could practice voice commands?
    - ii. Why did you decide not to practice the voice commands?
  - g. [If subject was shown Control condition]
    - i. How do you feel about practice voice commands that are focused on privacy? [show subject example of mobile app screen]
12. Is there anything else you would like to mention about your experience in the study today?

## References

- [1] “BBC - A History of the World - Object : HAL 9000 from 2001 - A Space Odyssey.” <https://www.bbc.co.uk/ahistoryoftheworld/objects/ZEXOQzEvQKSSbyvTodCA2A> (accessed Apr. 24, 2021).
- [2] S. Garfinkel, “Happy Birthday, Hal | WIRED,” Jan. 01, 1997. <https://www.wired.com/1997/01/ffhal/> (accessed Apr. 24, 2021).
- [3] Bethany Anderson, “The Birth of the Computer Age at Illinois,” *University of Illinois Archives*, Sep. 23, 2013. <https://archives.library.illinois.edu/blog/birth-of-the-computer-age/> (accessed Apr. 24, 2021).
- [4] “Use of Smart Speakers in the U.S. Increases During Quarantine,” *NPR.org*. <https://www.npr.org/about-npr/848319916/use-of-smart-speakers-in-the-u-s-increases-during-quarantine> (accessed Apr. 24, 2021).
- [5] D. J. Dubois, R. Kolcun, A. M. Mandalari, M. T. Paracha, D. Choffnes, and H. Haddadi, “When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers,” *Proc. Priv. Enhancing Technol.*, vol. 2020, no. 4, pp. 255–276, Oct. 2020, doi: 10.2478/popets-2020-0072.
- [6] A. Yichiet, J. Min, and G. Lee, “Pervasive Internet of Things (IoT) for Smart Speakers Discovery and Playback Continuity,” 2020, pp. 76–97.
- [7] R. Schmelzer, “Are Smart Speakers Really Smart?,” *Forbes*. <https://www.forbes.com/sites/cognitiveworld/2019/12/05/smart-speakers-dumb-term-for-an-intelligent-device/> (accessed Apr. 22, 2021).
- [8] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IoT Privacy and Security: Challenges and Solutions,” *Appl. Sci.*, vol. 10, no. 12, Art. no. 12, Jan. 2020, doi: 10.3390/app10124102.
- [9] S. Barth, M. D. T. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, “Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources,” *Telemat. Inform.*, vol. 41, pp. 55–69, Aug. 2019, doi: 10.1016/j.tele.2019.03.003.
- [10] E. Zeng and F. Roesner, “Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study,” p. 19.
- [11] A. Mhaidli, M. K. Venkatesh, Y. Zou, and F. Schaub, “Listen Only When Spoken To: Interpersonal Communication Cues as Smart Speaker Privacy Controls,” p. 20.
- [12] N. Abdi, K. M. Ramokapane, and J. M. Such, “More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants,” p. 17.
- [13] J. Lau, B. Zimmerman, and F. Schaub, “Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers,” *Proc. ACM Hum.-Comput. Interact.*, vol. 2, no. CSCW, pp. 1–31, Nov. 2018, doi: 10.1145/3274371.
- [14] Y. Huang, B. Obada-Obieh, and K. (Kosta) Beznosov, “Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks,” in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu HI USA, Apr. 2020, pp. 1–13, doi: 10.1145/3313831.3376529.

- [15]H. Chung and S. Lee, “Intelligent Virtual Assistant knows Your Life,” *ArXiv180300466 Cs*, Feb. 2018, Accessed: Apr. 22, 2021. [Online]. Available: <http://arxiv.org/abs/1803.00466>.
- [16]B. R. Cowan *et al.*, “‘What can i help you with?’: infrequent users’ experiences of intelligent personal assistants,” in *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services*, New York, NY, USA, Sep. 2017, pp. 1–12, doi: 10.1145/3098279.3098539.
- [17]A. Sciuto, A. Saini, J. Forlizzi, and J. I. Hong, “‘Hey Alexa, What’s Up?’: A Mixed-Methods Studies of In-Home Conversational Agent Usage,” in *Proceedings of the 2018 Designing Interactive Systems Conference*, New York, NY, USA, Jun. 2018, pp. 857–868, doi: 10.1145/3196709.3196772.
- [18]B. Sudharsan, M. I. Ali, and P. Corcoran, “Smart speaker design and implementation with biometric authentication and advanced voice interaction capability,” Dec. 2019.
- [19]E. McReynolds, S. Hubbard, T. Lau, A. Saraf, M. Cakmak, and F. 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*, New York, NY, USA, May 2017, pp. 5197–5207, doi: 10.1145/3025453.3025735.
- [20]F. Mccreary, A. Zafiroglu, and H. Patterson, “The Contextual Complexity of Privacy in Smart Homes and Smart Buildings,” Jul. 2016, vol. 9752, pp. 67–78, doi: 10.1007/978-3-319-39399-5\_7.
- [21]“Compare the Privacy Practices of the Most Popular Smart Speakers with Virtual Assistants,” *Common Sense Education*, Nov. 26, 2019. <https://www.commonsense.org/education/articles/compare-the-privacy-practices-of-the-most-popular-smart-speakers-with-virtual-assistants> (accessed Apr. 24, 2021).
- [22]K. Kumatani, J. McDonough, and B. Raj, “Microphone Array Processing for Distant Speech Recognition: From Close-Talking Microphones to Far-Field Sensors,” *IEEE Signal Process. Mag.*, vol. 29, no. 6, pp. 127–140, Nov. 2012, doi: 10.1109/MSP.2012.2205285.
- [23]B. Barrett, “What Amazon Echo and Google Home Do With Your Voice Data—And How to Delete It,” *Wired*.
- [24]L. Manikonda, A. Deotale, and S. Kambhampati, “What’s up with Privacy? User Preferences and Privacy Concerns in Intelligent Personal Assistants,” in *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society*, New York, NY, USA, Dec. 2018, pp. 229–235, doi: 10.1145/3278721.3278773.
- [25]H. Chen, F. Li, and Y. Wang, “EchoTrack: Acoustic device-free hand tracking on smart phones,” in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, May 2017, pp. 1–9, doi: 10.1109/INFOCOM.2017.8057101.
- [26]A. Pradhan, K. Mehta, and L. Findlater, “‘Accessibility Came by Accident’: Use of Voice-Controlled Intelligent Personal Assistants by People with Disabilities,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, Apr. 2018, pp. 1–13, doi: 10.1145/3173574.3174033.
- [27]“Set up and manage Routines - Android - Google Nest Help.” <https://support.google.com/googlenest/answer/7029585?co=GENIE.Platform%3DAndroid&hl>

- =en#zippy=%2Cgood-morning (accessed Apr. 22, 2021).
- [28]R. W. White, "Skill discovery in virtual assistants," *Commun. ACM*, vol. 61, no. 11, pp. 106–113, Oct. 2018, doi: 10.1145/3185336.
- [29]Br, on V. in I. of T. on October 8, 2020, and 12:50 Pm Pst, "Google Nest smart speakers: A cheat sheet," *TechRepublic*.  
<https://www.techrepublic.com/article/google-nest-smart-speakers-a-cheat-sheet/> (accessed Apr. 22, 2021).
- [30]F. Eriksson, "Onboarding Users to a Voice User Interface," p. 75.
- [31]S. Hulick, "User Onboarding | A frequently-updated compendium of web app first-run experiences," *UserOnboard*. <https://www.useronboard.com/> (accessed Apr. 24, 2021).
- [32]"The ultimate guide to user onboarding." <https://www.appcues.com/user-onboarding> (accessed Apr. 24, 2021).
- [33]"An intro to user onboarding, part 1 | Inside Design Blog."  
[https://www.invisionapp.com/inside-design/an\\_intro\\_to\\_user\\_onboarding\\_part\\_1/](https://www.invisionapp.com/inside-design/an_intro_to_user_onboarding_part_1/) (accessed Apr. 24, 2021).
- [34]"Mobile Onboarding: A Beginner's Guide," *Smashing Magazine*.  
<https://www.smashingmagazine.com/2014/08/mobile-onboarding-beginners-guide/> (accessed Apr. 24, 2021).
- [35]C. Pearl, *Designing Voice User Interfaces: Principles of Conversational Experiences*. O'Reilly Media, Inc., 2016.
- [36]R. R. Burke, "Technology and the Customer Interface: What Consumers Want in the Physical and Virtual Store," *J. Acad. Mark. Sci.*, vol. 30, no. 4, pp. 411–432, Oct. 2002, doi: 10.1177/009207002236914.
- [37]J. Hakulinen, M. Turunen, and E.-P. Salonen, "Software Tutors for Dialogue Systems," in *Text, Speech and Dialogue*, vol. 3658, V. Matoušek, P. Mautner, and T. Pavelka, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 412–419.
- [38]O. Michler, R. Decker, and C. Stummer, "To trust or not to trust smart consumer products: a literature review of trust-building factors," *Manag. Rev. Q.*, vol. 70, Sep. 2019, doi: 10.1007/s11301-019-00171-8.
- [39]M. T. Dzindolet, S. A. Peterson, R. A. Pomranky, L. G. Pierce, and H. P. Beck, "The role of trust in automation reliance," *Int. J. Hum.-Comput. Stud.*, vol. 58, no. 6, pp. 697–718, Jun. 2003, doi: 10.1016/S1071-5819(03)00038-7.
- [40]H. Abraham, "1 AUTONOMOUS VEHICLES AND ALTERNATIVES TO DRIVING: TRUST, 2 PREFERENCES, AND EFFECTS OF AGE," p. 16, 2017.
- [41]G. Dominici, V. Roblek, T. Abbate, and M. Tani, "Click and drive: consumer attitude to product development. Towards future transformations of the driving experience," *Bus. Process Manag. J.*, vol. 22, no. 2, Jan. 2016, doi: 10.1108/BPMJ-05-2015-0076.
- [42]D. Wright, "The dark side of ambient intelligence," *info*, vol. 7, pp. 33–51, Dec. 2005, doi: 10.1108/14636690510628300.
- [43]M. J. Cronin, *Smart Products, Smarter Services: Strategies for Embedded Control*. Cambridge University Press, 2010.



- [44] A. J. B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon, "Home automation in the wild: challenges and opportunities," in *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, Vancouver, BC, Canada, 2011, p. 2115, doi: 10.1145/1978942.1979249.
- [45] R. Yang and M. Newman, "Learning from a learning thermostat: Lessons for intelligent systems for the home," Sep. 2013, pp. 93–102, doi: 10.1145/2493432.2493489.
- [46] E. M. Rogers, *Diffusion of Innovations, 5th Edition*. Riverside, UNITED STATES: Free Press, 2003.
- [47] K. Park, C. Kwak, J. Lee, and J.-H. Ahn, "The effect of platform characteristics on the adoption of smart speakers: Empirical evidence in South Korea," *Telemat. Inform.*, vol. 35, no. 8, pp. 2118–2132, Dec. 2018, doi: 10.1016/j.tele.2018.07.013.
- [48] A. H. Eichelberger and A. T. McCartt, "Toyota drivers' experiences with Dynamic Radar Cruise Control, Pre-Collision System, and Lane-Keeping Assist," *J. Safety Res.*, vol. 56, pp. 67–73, Feb. 2016, doi: 10.1016/j.jsr.2015.12.002.
- [49] E. Beneteau *et al.*, "Assumptions Checked: How Families Learn About and Use the Echo Dot," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 4, no. 1, pp. 1–23, Mar. 2020, doi: 10.1145/3380993.
- [50] E. Corbett and A. Weber, "What can I say?: addressing user experience challenges of a mobile voice user interface for accessibility," in *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services*, Florence Italy, Sep. 2016, pp. 72–82, doi: 10.1145/2935334.2935386.
- [51] Y. Yao, J. R. Basdeo, S. Kaushik, and Y. Wang, "Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, May 2019, pp. 1–12, doi: 10.1145/3290605.3300428.
- [52] C. Geeng and F. Roesner, "Who's In Control? Interactions In Multi-User Smart Homes," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, May 2019, pp. 1–13, doi: 10.1145/3290605.3300498.
- [53] N. Malkin, J. Deatrack, A. Tong, P. Wijesekera, S. Egelman, and D. Wagner, "Privacy Attitudes of Smart Speaker Users," *Proc. Priv. Enhancing Technol.*, vol. 2019, no. 4, pp. 250–271, Oct. 2019, doi: 10.2478/popets-2019-0068.
- [54] A. Weiss, R. Bernhaupt, D. Schwaiger, M. Altmaninger, R. Buchner, and M. Tscheligi, "User experience evaluation with a Wizard of Oz approach: Technical and methodological considerations," in *2009 9th IEEE-RAS International Conference on Humanoid Robots*, Dec. 2009, pp. 303–308, doi: 10.1109/ICHR.2009.5379559.
- [55] E. Luger and T. Rodden, "An informed view on consent for UbiComp," in *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, Zurich Switzerland, Sep. 2013, pp. 529–538, doi: 10.1145/2493432.2493446.
- [56] "Alexa, she's not human but... Unveiling the drivers of consumers' trust in voice-based artificial intelligence - Pitardi - 2021 - Psychology & Marketing - Wiley Online Library." <https://onlinelibrary-wiley-com.proxy.lib.umich.edu/doi/full/10.1002/mar.21457> (accessed Apr.

24, 2021).

- [57] J. Sweller, "CHAPTER TWO - Cognitive Load Theory," in *Psychology of Learning and Motivation*, vol. 55, J. P. Mestre and B. H. Ross, Eds. Academic Press, 2011, pp. 37–76.
- [58] V. Koshy, J. S. Park, T.-C. Cheng, and K. Karahalios, "'We Just Use What They Give Us': Understanding Passenger User Perspectives in Smart Homes," p. 22, 2021.
- [59] "Bounded Rationality - Biases & Heuristics," *The Decision Lab*.  
<https://thedecisionlab.com/biases/bounded-rationality/> (accessed Apr. 24, 2021).
- [60] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Secur. Priv. Mag.*, vol. 3, no. 1, pp. 26–33, Jan. 2005, doi: 10.1109/MSP.2005.22.
- [61] D. J. Solove, "INTRODUCTION: PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA," *Harv. Law Rev.*, vol. 126, no. 7, pp. 1880–1903, 2013.
- [62] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A Design Space for Effective Privacy Notices\*," in *The Cambridge Handbook of Consumer Privacy*, 1st ed., E. Selinger, J. Polonetsky, and O. Tene, Eds. Cambridge University Press, 2018, pp. 365–393.
- [63] L. Curren and J. Kaye, "Revoking consent: A 'blind spot' in data protection law?," *Comput. Law Secur. Rev.*, vol. 26, no. 3, pp. 273–283, May 2010, doi: 10.1016/j.clsr.2010.03.001.
- [64] A. Morrison, D. McMillan, and M. Chalmers, "Improving consent in large scale mobile HCI through personalised representations of data," in *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, Helsinki Finland, Oct. 2014, pp. 471–480, doi: 10.1145/2639189.2639239.
- [65] L. Lee and J. D. Still, "Re-designing Permission Requirements to Encourage BYOD Policy Adherence," in *Human Aspects of Information Security, Privacy, and Trust*, Cham, 2015, pp. 369–378, doi: 10.1007/978-3-319-20376-8\_33.
- [66] "OECD Privacy Guidelines - OECD."  
<https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm> (accessed Apr. 24, 2021).
- [67] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User Perceptions of Smart Home IoT Privacy," *Proc. ACM Hum.-Comput. Interact.*, vol. 2, no. CSCW, pp. 1–20, Nov. 2018, doi: 10.1145/3274469.
- [68] T. Ammari, J. Kaye, J. Y. Tsai, and F. Bentley, "Music, Search, and IoT: How People (Really) Use Voice Assistants," vol. 26, no. 3, p. 28.
- [69] F. Schaub and L. F. Cranor, *An introduction to privacy for technology professionals*. Portsmouth, NH: International Association of Privacy Professionals, 2020.
- [70] "Amazon.com Help: Ask Alexa to Delete Your Voice History."  
<https://www.amazon.com/gp/help/customer/display.html?nodeId=GYRPHMGANH7M2BNH> (accessed Apr. 24, 2021).
- [71] "• Global smart speaker market share 2020 | Statista."  
<https://www.statista.com/statistics/792604/worldwide-smart-speaker-market-share/> (accessed Apr. 24, 2021).
- [72] "Google Nest Smart Speakers & Displays - Google Store."  
[https://store.google.com/us/magazine/compare\\_nest\\_speakers\\_displays](https://store.google.com/us/magazine/compare_nest_speakers_displays) (accessed Apr. 24, 2021).
- [73] "Amazon.com: Echo Smart Speakers & Displays: Amazon Devices & Accessories: Smart Speakers,

Smart Displays & More.”

<https://www.amazon.com/smart-home-devices/b?ie=UTF8&node=9818047011> (accessed Apr. 24, 2021).

[74] L. Feiner, “Google U.S. ad revenue will drop for the first time this year, eMarketer says,” *CNBC*, Jun. 22, 2020.

<https://www.cnn.com/2020/06/22/google-ad-revenue-will-drop-this-year-emarketer-says.html> (accessed Apr. 24, 2021).

[75] “FAQs on privacy: Google Nest - Android - Google Nest Help.”

[https://support.google.com/googlenest/answer/9415830?p=privacyfaqs&hl=en&visit\\_id=637411439754338942-2705115295&rd=1#zippy=%2Care-my-assistant-voice-queries-used-to-inform-ad-personalization](https://support.google.com/googlenest/answer/9415830?p=privacyfaqs&hl=en&visit_id=637411439754338942-2705115295&rd=1#zippy=%2Care-my-assistant-voice-queries-used-to-inform-ad-personalization) (accessed Apr. 24, 2021).

[76] “Gunning Fog Index.” <http://gunning-fog-index.com/> (accessed Apr. 24, 2021).

[77] “Readability and the Gunning Fog Index,” *Readable*, Mar. 27, 2017.

<https://readable.com/blog/the-gunning-fog-index/> (accessed Apr. 24, 2021).

[78] B. B. Anderson, A. Vance, C. B. Kirwan, J. L. Jenkins, and D. Eargle, “From Warning to Wallpaper: Why the Brain Habituates to Security Warnings and What Can Be Done About It,” *J. Manag. Inf. Syst.*, vol. 33, no. 3, pp. 713–743, Jul. 2016, doi: 10.1080/07421222.2016.1243947.

[79] “What Google’s Material Design Is Really About | WIRED.”

<https://www.wired.com/insights/2014/12/google-material-design/> (accessed Apr. 24, 2021).

[80] “What is Material Design?,” *The Interaction Design Foundation*.

<https://www.interaction-design.org/literature/topics/material-design> (accessed Apr. 24, 2021).

[81] P. Emami-Naeini *et al.*, “Privacy Expectations and Preferences in an IoT World,” p. 15.

[82] “Data security and privacy on devices that work with Assistant - Google Nest Help.”

<https://support.google.com/googlenest/answer/7072285?hl=en> (accessed Apr. 24, 2021).

[83] Adobe, “Design voice prototypes.”

<https://helpx.adobe.com/xd/user-guide.html/xd/help/voice-prototypes-in-adobe-xd.ug.html> (accessed Apr. 24, 2021).

[84] “‘Hey Google, Open Adobe XD’: Test voice prototypes on Google Assistant devices,” *Adobe Blog*, Oct. 28, 2020.

<https://blog.adobe.com/en/publish/2020/10/28/test-xd-voice-prototypes-google-assistant-plugin.html> (accessed Apr. 24, 2021).

[85] “Prolific | Online participant recruitment for surveys and market research.”

<https://www.prolific.co/> (accessed Apr. 24, 2021).

[86] “ProtoPie | The interactive digital prototyping tool,” *ProtoPie*. <https://www.protopie.io/> (accessed Apr. 24, 2021).

[87] “Free Lottie Animation Files, Tools & Plugins - LottieFiles.” <https://lottiefiles.com/> (accessed Apr. 24, 2021).

[88] N. A. Draper, “From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates,” *Policy Internet*, vol. 9, no. 2, pp. 232–251, 2017, doi:

<https://doi.org/10.1002/poi3.142>.

[89] D. H. Mortensen, “How to Do a Thematic Analysis of User Interviews,” *The Interaction Design*

*Foundation.*

<https://www.interaction-design.org/literature/article/how-to-do-a-thematic-analysis-of-user-interviews> (accessed Apr. 24, 2021).

- [90] G. B. Willis and A. R. Artino, "What Do Our Respondents Think We're Asking? Using Cognitive Interviewing to Improve Medical Education Surveys," *J. Grad. Med. Educ.*, vol. 5, no. 3, pp. 353–356, Sep. 2013, doi: 10.4300/JGME-D-13-00154.1.
- [91] "Capitalize My Title," *Capitalize My Title*. <https://capitalizemytitle.com/page-count/> (accessed May 06, 2021).