Understanding User Perceptions of Voice Personal Assistants

Ha Young Kim
hayounk@clemson.edu

Follow this and additional works at: https://tigerprints.clemson.edu/all_theses

Part of the Computer Sciences Commons

Recommended Citation
Kim, Ha Young, "Understanding User Perceptions of Voice Personal Assistants" (2022). All Theses. 3742. https://tigerprints.clemson.edu/all_theses/3742

This Thesis is brought to you for free and open access by the Theses at TigerPrints. It has been accepted for inclusion in All Theses by an authorized administrator of TigerPrints. For more information, please contact kokeefe@clemson.edu.
UNDERSTANDING USER PERCEPTIONS OF
VOICE PERSONAL ASSISTANTS

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial fulfillment
of the Requirements for the Degree
Master of Science
Computer Science

by
Ha Young Kim
May 2022

Accepted by:
Dr. Long Cheng, Committee Chair
Dr. Nina Hubig
Dr. Feng Luo
Abstract

As the artificial intelligence (AI) technique improves, voice assistant (smart speaker) such as Amazon Alexa and Google Assistant are quickly, surely permeating into people’s daily lives. With its powerful and convenient benefits and the circumstances that people started to stay at their home longer due to the pandemic, reliance on smart speakers has increased rapidly. But at the same time, concerns of security on smart speakers have increased.

In this thesis, we conducted an online user survey of smart speaker users with five different perspectives – 1) Users’ engagement with privacy policy; 2) Awareness of different policy requirements defined by smart speaker providers; 3) User’s concerns in multi-user environment; 4) Developer’s perception of general policies; and 5) Social biases of speech recognition on smart speaker (Fairness). With the survey, we could reveal the users’ expectations on smart speakers and their difficulties in several situations, developer’s perception, developer's difficulties on generating privacy policy and meeting conditions for each application. Interestingly, some participants showed satisfaction overall and had perception about both the appropriate privacy policy and policy requirements, but there were quite a few people who read the privacy policy and had a lot of concerns. All participants were asking for speaker recognition even though the VPA devices provides the feature already. Also, many users have experienced low accuracy of speech recognition and some of them have noticed that age, gender, race, and dialects have different effects on smart speakers understanding their commands.
Acknowledgments

First of all, as I had challenges of changing the topic, I really appreciate my thesis advisor, Dr. Long Cheng for his attentive guidance and advice throughout the process of the research and writing this thesis. I appreciate the rest of my committee members, Dr. Nina Hubig and Dr. Feng Luo for their interest and help through this process. Second, I would like to thank for member of Dr. Cheng’s lab, Song Liao for his assistance and feedback on my thesis.

Also, I would like to thank the faculty and staff of Computer Science department for providing me the chance for graduate study and supports throughout my academic life at Clemson University.

Finally, I would like to thank my family and friends, for their endless support and encouragement on my entire challenges for my graduate study.
# Table of Contents

Title Page ......................................................... i  
Abstract ......................................................... ii  
Acknowledgments ................................................ iii  
List of Tables .................................................... vi  
List of Figures ................................................... vii  

1 Introduction .................................................. 1  
  1.1 Motivation ................................................... 3  

2 Background and Related Works ............................... 7  
  2.1 Voice Personal Assistant ................................... 7  
  2.2 Policy Requirements of VPA Platform ...................... 9  
  2.3 Privacy and Security Concerns on Smart Speakers .......... 9  
  2.4 Developers of VPA ........................................ 13  
  2.5 Social Bias of Smart Speaker ............................. 15  
  2.6 Focused Problems ......................................... 15  

3 Methods ......................................................... 17  
  3.1 Recruitment ................................................ 17  
  3.2 Purpose of the Study ...................................... 18  

4 Results and Findings ........................................ 22  
  4.1 General Usage ............................................. 22  
  4.2 Both VPA User’s and Developer’s Issue .................... 22  
  4.3 Issues Encountered by VPA Users ......................... 24  
  4.4 Issues with VPA Developers ............................... 31  
  4.5 VPA System Issue ......................................... 34  
  4.6 Limitations ................................................. 35  

5 Discussion and Conclusion .................................. 41  
  5.1 Discussion ................................................ 41  
  5.2 Conclusion ................................................. 43
List of Tables

2.1 List of restriction content policies on Google ......................... 10
2.2 List of restriction content policies on Amazon ........................ 11

4.1 Awareness survey questions and % of responses ....................... 23
4.2 Privacy policy survey questions and % of responses .................... 26
4.3 Multi-user survey questions and % of responses ....................... 38
4.4 Developer survey questions and % of responses ....................... 39
4.5 Fairness survey questions and % of responses ........................ 40
List of Figures

2.1 Architecture of VPA service ........................................ 8
2.2 Problem Highlight ...................................................... 16

4.1 User’s scaled awareness of smart speaker features .......... 24
4.2 Users’ perception on privacy policy ................................ 27
4.3 User’s scaled perception on guest using their smart speaker 29
4.4 User’s scaled perception on stranger accessing personal information by smart speaker 29
4.5 User’s scaled perception on parent-kids environment .......... 30
4.6 Developers’ scaled perspective on privacy policy ............. 32
4.7 Developers’ scaled perspective on privacy policy and voice-app rate 33
4.8 Developers’ scaled perspective on privacy policy generating program 34
Chapter 1

Introduction

Since Artificial Intelligence appeared, AI-based techniques quickly settled on our real lives. Among them, the Smart Assistance system is the most common technology that people can access. This system became common after Apple Siri, Samsung Bixby, Microsoft Cortana, the technique such as smart mobile environments were distributed. Now they are coming out and increasing rapidly with the appearance of smart speakers (as known as voice personal assistants) due to its convenience benefits. The global smart speakers’ market is expected to grow from $4.66 billion in 2020 to $6.98 billion in 2021 at a compound annual growth rate (CAGR) of 49.8%. The smart speaker market is expected to reach $17.85 billion in 2025, at a CAGR of 26% [1]. Despite of supply chain challenges, component shortages due to COVID-19 pandemic circumstances, global smart speaker sales has increased [2].

The smart speaker provides hand-free and personalized information assistant. Consumers can use it as smart home device controller to lock the door or turn on the light or using as a personal routine assistant like getting weather updates, notification of calendar event, setting a reminder or alarm. Voice Personal Assistant (VPA) platforms allow third-party developers to publish their skills or actions (Amazon platform calls voice-app as skills and Google platform calls them as actions, we would simply call it as voice-app for now on) to the voice-app stores. So, consumers can search about third-party voice-apps simply by asking for a request, asking a question to smart speaker [3].
The two mainstream of VPA devices are Amazon Alexa and Google Assistant, each of the devices can link users’ accounts so users can search their interests and do shopping with their voice control. The biggest benefit of using smart speaker is that it offers user hands-free control with their voice, to use the device, user must use 'wake word' for each smart speaker (e.g., for Amazon Alexa, the user has to call "Alexa" before asking for the voice-app. These wake words can be modified by the user) [3]. As shown on the previous research [4], they’ve found existence of voice-app that has a lack of privacy policy or broken privacy policy, or incorrect privacy policy on VPA voice-app market. A privacy policy is a statement or legal document that distinguishes the ways a party gathers, uses, discloses, and manages customer’s personal data [5], which should be provided by voice-app developers when they collect user’s personal data. Despite the much longer service of the mobile application market, it has similar issues with VPA voice-app market. From the previous studies [6] and [7], researchers have shown that even several official mobile applications are providing invalid privacy policies and concerning of the risks caused by it. Such issues pose challenges on effective privacy notices to enable users to make informed privacy decisions. This motivated us to conduct a user study to understand users’ engagement of privacy policy on voice-app.

The biggest factor of non-user for not adopting the smart speaker is mostly users’ security and privacy concerns [8]. Most VPA devices have a basic speaker shape without a display panel. Consumer’s control to use the VPA device is limited to their voices, which makes them hard to use it meticulously such as checking the log or other debugging features from the device. Also, unlike other environments that has display such as mobile phone, the smart speakers can be used by multiple users and connected to multiple accounts. Due to those features, the risk of using VPA devices such as privacy or security problems arose. Though smart speakers have a similar environment with mobile’s VPA, smart speaker is hard to notify each voice-app’s privacy policy and what type of personal data voice-app collects and it is even hard to notice exact voice-app is executed without using other devices, which makes attack easier and made smart speakers more vulnerable than the mobile environment.
Previous study by Edu et al. [9] has shown a lot of consumers are concerned with VPA device’s authentication or authorization. Another concern from user is that smart speaker uses microphone to capture their command and risk of hacking on device’s cloud storage that has record of their use. Researchers found that Amazon’s smart home devices could have allowed hackers access to personal information and record of conversations between the user and device [10, 11]. According to the article, the attacker could get a list of installed voice-apps using a malicious Amazon link and steal a token allowing them to add or remove skills. Or the attacker could install a malicious skill that uses same series of spoken words to trigger the voice-apps (the ‘invocation phrase’) and remove the original one. Also, microphones are one of the most problematic sensors for privacy [8]. Regardless of the manufacturers’ claim that their devices don’t store all the conversation and the device is designed to respond only with invocation phrases, the existence of microphones can make consumers have concerns about it.

For Amazon Alexa, user can activate smart speaker’s features by asking their devices directly to the device. Consumers’ requests are routed to the designated data source where information is gathered and provide the voice-app that user asked [12]. While doing the process, the device can activate malicious voice-app that wasn’t users’ expectation or use different voice-app that can share its users’ information with third parties. Since smart speaker are usually connected with consumer’s personal account, it can cause serious security problems such as personal information leakage. Despite all those security and privacy concerns that consumers have with VPA devices, the benefits of using the devices are strong, which makes adopting the device to be common.

1.1 Motivation

To improve users’ usability of the VPA devices, prior studies have focused on understanding users’ experience with several surveys. Edu et al. [9], Lau et al. [8], Abdi et al. [13], Manikonda et al. [14], Cho et al. [15], Emami et al. [16, 17] and Ponticello et al. [18]
have studied about several security and privacy issues on VPA devices. Zeng et al. [19], Jang et al. [20], Huang et al. [21] and Geeng et al. [22] have mainly studied privacy issues and user’s concern on multi-user situations. Feng et al.[23], Liu et al. [24], Martin et al. [25], Koenecke et al. [26], Fenu et al. [27] have found social bias issues on automatic speech recognition modules in VPA. To understand users’ perception or concerns and to improve usability of VPA device, we conducted a user studies from 5 different perspectives - Users’ perception on privacy policy, Users’ awareness of different policies from several category of the market, Users’ concern and usability on multi-user environment, Developer’s difficulty and perception of market’s policy, and Biases of social factors while using the smart speaker.

A privacy policy is a statement or legal document that distinguishes the ways a party gathers, uses, discloses, and manages customer’s personal data. Personal data can be anything that can be used to identify an individual, including person’s name, address, contact information, financial records, etc [5]. If the application collects personal data, developers have to provide a privacy policy and notify it to users about their application’s privacy practices. The VPA device’s features are easy to use regardless of age, but unfortunately, it is difficult to check immediately whether voice-apps provides adequate privacy policies for users while using them because most of the smart speakers direct users to voice-app detail web page via other devices. Voice-app markets do not check meticulously the existence of an exact privacy policy or make it essential for developers to submit their voice-app even though market requires certification process, which made applications have a lack of privacy policies or allowed to have wrong privacy policy. So, we conducted a survey to collect experiences how users engage with privacy policies of voice-apps, and to understand users’ frustrations regarding privacy notice of voice-apps and their perspectives on it.

Amazon Alexa and Google Assistant are two main stream VPA platforms. Each of them has unique policy requirements such as for Amazon, if the voice-app collects personal data from end users, the voice-app must display a legally adequate privacy policy within the app and on the app detail page [28]. For Google, they requires all Actions to post a link to their privacy policy in the Directory of their cloud [29]. Also, there are different policies
required by category even on the same market. For example, on kids’ category, voice-app
cannot include the content that is not suitable for children. Recent studies show many voice-
app that violates policy exists on the marketplace today. For instance, SkillDetective [30]
identified 6,254 voice-apps potentially violating at least one policy requirement. [4] identified
38% of Google voice-app has missing privacy policy and 9% of duplicate privacy policy
URLs, 28% of Amazon voice-app has missing privacy policy and 56% of duplicate privacy
policy URLs. SkillExplorer [31] identified 1,141 voice-app request users’ personal information
without following the VPA platform’s developer specifications. We are curious whether users
and developers are aware of various policy restrictions and requirements defined by VPA
platforms. To identify, we conducted a user study to understand uses'/developers’ perception
of these policy restrictions and requirements.

Due to its features such as answering questions, VPA devices are usually placed in
central location of home or intersection points of multiple rooms so all house members can
access [8]. The users could be a family member of adults or with kids, guests, housemates,
and more. There could be a security risk because of this diversity, the previous research
from Zeng et al. [19] showed power imbalance exists between primary users and secondary
(non-primary) users. As the VPA devices are expected to be used with multiple consumers
in one place, the need of a fine-grained multi-user access control for smart speaker users
has appeared.

The developer must consider more features and has a different perspective compared
to general users. Also, they must provide adequate privacy policy for voice-app users because
they are providing content for users. But as the previous study from Song et al. [4], a lot of
voice-apps have duplicate privacy policy or the description of the voice-app and the actual
privacy policy document do not corresponds or don’t provide it. Also, Le et al [32] found that
a lot of voice-apps violate required policy for kids’ category which has specific requirements
and includes risky contents on Alexa market. To identify the fundamental cause on lack
of privacy violations in the current voice-app stores, we wanted to know the developer’s
perception, difficulties, and awareness of privacy policy requirement and restrictions of the
VPA platform market.

There are also social biases on VPA services but not a lot of users know about it. VPA devices use Automatic Speech Recognition (ASR) and Natural Language Understanding (NLU) to understand and translate human acoustic signal (voice command) to word sequence so device can understand it digitally. Each individual’s voice is unique, it contains information that can specify the type of person such as gender, age, spoken language (speaking habitual) due to shape of chest and neck or the position of the tongue [33]. But ASR and NLU is not as accurate and flexible on understanding the acoustic signal as human. Because of this, even the users ask for the same actions, the results could be differed by gender, race, and age. So, we wanted to get user experiences and perceptions on fairness of speaker recognition and speech recognition in smart speakers.
Chapter 2

Background and Related Works

In this section, we will first discuss VPA background and summarize the previous papers that researched users’ privacy, multi-user privacy, fairness on VPA.

2.1 Voice Personal Assistant

Voice Personal Assistant (VPA) is a software agent that can perform tasks or services based on commands or questions of the individual’s voices [34]. The smart speakers such as Amazon Alexa or Google Assistant use cloud-based system. Figure 2.1 shows the basic architecture of VPA service. For Alexa, if user request a voice command to VPA with their voice including wake word, the VPA detects customer’s request and send it to service provider’s cloud server translating the voice into text by using ASR (Automatic Speech Recognition). ASR is a technology that converts spoken words into text, which allows VPA devices to detect spoken sounds from user and recognize them as words [35]. After ASR process, NLU (Natural Language Understanding) process starts, which allows computers to deduce what a user actually means and makes users feel like having an actual conversation [36]. By using NLU, it assigns meaning to text so the request can be routed to the designated data source and by using Text-To-Speech (TTS), the device generates voice responds for user. Also, for user’s convenience, VPA devices provide third-party skills that can be executed on
the device. The VPA platform market has different privacy policy requirements due to its specialty, Google requires every action to have a privacy policy and Amazon requires skills that collect personal information only to mandatorily have a privacy policy [4].

Voice Personal Assistant’s voice-app has front-end interface and back-end code to manage how it responds to user requests. The front-end interface for voice-app is hosted by VPA device’s cloud, but back-end code is hosted on the developer’s server. Each voice-app should have unique way to invoke, made to verbally interactive and return audible response [30]. The voice-app markets allow third-party developers to submit their own voice-app. The voice-app developers usually follow the workflow - designing the voice-app, build the voice-app, test the voice-app, get certified, publish the voice-app on market, manage the voice-app after publish. VPA device platforms require each voice-app to get certification before publishing the voice-app.
2.2 Policy Requirements of VPA Platform

For Google Assistant’s privacy policy, they stated to accurately describe its specific Action (voice-app). It must contain what information Action collects, how does it use the information and what information would Action share. Also, there are content restrictions such as they do not allow Actions to contain or promote sexual content or any content or services intended to be sexually gratifying, to depict or facilitate gratuitous violence or other dangerous activities. They recommend using Google Sites to create a new site for privacy policy field so developer can use it when they publish an Action [37].

For Amazon’s privacy policy, skills can only collect and use the data required to support and improve the features and services it provides and should display a legally adequate privacy policy within the app and on the app detail page. Also, the privacy policy must comprehensively disclose what personal data that skill collects, how it is used, and the types of parities with whom it is shared. Amazon also has content restriction policy that is similar with Google, such as if the skill contains content that would not be considered ‘family-friendly’ and does not have adequate safeguards in place for young users it will be rejected and applications containing pornography or that depict sexual acts or sexually explicit material is prohibited [38]. The lists of the representative restriction policies on two platforms are shown in Table 2.1 and Table 2.2.

2.3 Privacy and Security Concerns on Smart Speakers

A lot of studies have done to figure out privacy and security concerns and user’s perceptions on smart speakers. Edu et al. [9] have investigated users’ security and privacy concerns on general VPA devices such as weak authentication that wake word is the only way to authenticate the user, and weak payment authorization that while users use their device for online shopping, the restriction after PIN code lockout is not defined. Due to the weak authorization for shopping, even children can shop with VPA devices to fulfill their desires so cases such as parents find out getting several order confirmation emails they
<table>
<thead>
<tr>
<th>Platform</th>
<th>Restrictions</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>Sexually explicit</td>
<td>Contain or promote sexual content or services intended to be sexually gratifying</td>
</tr>
<tr>
<td></td>
<td>Child endangerment</td>
<td>Child sexual abuse content or promoting sexual exploitation of minors</td>
</tr>
<tr>
<td></td>
<td>Violence and dangerous activities</td>
<td>Depict or facilitate gratuitous violence or other dangerous activities (e.g., self-harm, suicide, choking games or other acts may result serious injury or death)</td>
</tr>
<tr>
<td></td>
<td>Bullying and harassment</td>
<td>Contain or facilitate threats, harassment, or bullying</td>
</tr>
<tr>
<td></td>
<td>Hate speech</td>
<td>Facilitate or promote content that advocates hate or violence or promotes discrimination against groups of people based on their race or ethnic origin, religion, disability, gender, age, nationality, veteran status, sexual orientation, gender identity, or any other characteristic that is associated with systemic discrimination or marginalization</td>
</tr>
<tr>
<td></td>
<td>Sensitive events</td>
<td>Lack reasonable sensitivity towards, or capitalize on, a natural disaster, pandemic, atrocity, conflict, death, or other tragic event</td>
</tr>
<tr>
<td></td>
<td>Gambling, games, and contests</td>
<td>Containing content or services that allow users to wager, stake, or participate using real money to obtain a prize of real-world monetary value</td>
</tr>
<tr>
<td></td>
<td>Illegal activities</td>
<td>Facilitate or promote illegal activities</td>
</tr>
<tr>
<td></td>
<td>Alcohol, tobacco drugs</td>
<td>Facilitate or promote the sale of alcohol are allowed only in countries listed in Google’s Alcohol Ads policy</td>
</tr>
<tr>
<td></td>
<td>Health</td>
<td>Involve transmission of information that could be considered protected health information under the Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td></td>
<td>Financial services</td>
<td>Expose users to deceptive or harmful financial products and services</td>
</tr>
<tr>
<td></td>
<td>Emergency services</td>
<td>Enable users to contact emergency responders, such as 911 or 999 services</td>
</tr>
</tbody>
</table>

Table 2.1: List of restriction content policies on Google
<table>
<thead>
<tr>
<th>Platform</th>
<th>Restrictions</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>Family-friendly</td>
<td>Contains content that would not be considered as &quot;family-friendly&quot; and does not have adequate safeguards in place for young customers</td>
</tr>
<tr>
<td></td>
<td>Sexually explicit</td>
<td>Containing pornography or that depict sexual acts or sexually explicit material</td>
</tr>
<tr>
<td></td>
<td>Violence and dangerous activities</td>
<td>Incite violence or contain excessive depictions of violence</td>
</tr>
<tr>
<td></td>
<td>Hate speech</td>
<td>Contain derogatory comments or hate speech specifically targeting any groups, individuals, religions, or nationalities</td>
</tr>
<tr>
<td></td>
<td>Harassment</td>
<td>Promote or contain harassment, bullying or threats</td>
</tr>
<tr>
<td></td>
<td>Sensitive events</td>
<td>Do not demonstrate reasonable sensitivity towards tragic events (historic and current), disasters or conflicts</td>
</tr>
<tr>
<td></td>
<td>Alcohol, tobacco</td>
<td>Promote the sale of alcohol or tobacco, contain underage use of tobacco or alcohol, or promote excessive use of alcohol or tobacco</td>
</tr>
<tr>
<td></td>
<td>Real-money gambling, gaming, and</td>
<td>Only listed countries can be allowed with heavily regulated with requirements</td>
</tr>
<tr>
<td></td>
<td>competitions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bitcoins and other crypto currencies</td>
<td>Facilitate the transaction of cryptocurrencies</td>
</tr>
<tr>
<td></td>
<td>Illegal activities</td>
<td>Promote or facilitate illegal activities</td>
</tr>
<tr>
<td></td>
<td>Regionally restricted</td>
<td>Content that would violate that country or region’s laws, cultural norms, or sensitivities</td>
</tr>
<tr>
<td></td>
<td>User-generated</td>
<td>Unmoderated</td>
</tr>
<tr>
<td></td>
<td>Medical Content</td>
<td>False claims regarding medicine and/or prescription drugs, purport to be able to predict the gender of a fetus</td>
</tr>
</tbody>
</table>

Table 2.2: List of restriction content policies on Amazon

didn’t order was because their children were doing a shopping with Alexa at home [39] can happen. Lau et al. [8] conducted a study for privacy concerns on general IoT (Internet of Things) devices, not only for smart speakers by implementing survey. They found out the positive factors of adoption is mainly due to the convenience of smart speaker, but the negative factors are lack of utility and privacy and security concerns. Through the study, they found that users usually place their device at intersection points of multiple rooms so all the households can access it easily, and the participants usually use their smart speaker with daily uses (checking weather, setting timers or reminders or calendar, asking questions,
controlling other devices, purchasing items, playing music). By the survey, they could also find most of participants concerns with targeting advertising issue, but some participants were unawareness on privacy-convenience trade-off. Abdi et al. [13] did a user survey on 43 customers who are using Amazon Alexa or Google Assistant. They studied about user’s perceptions of VPA ecosystem including third-party, shopping and data sharing issues. They found out that the users perceived that it is the device manufactures responsibility to protect users’ privacy. Emami et al. [16] has investigated about general IoT device’s privacy and security. They asked experts for labeling the IoT devices’ privacy and security factors and checked its effectiveness by doing a survey with non-experts. Also, for later work [17], they studied about the consumer’s factor of purchasing the IoT devices. They found that consumers are not aware of privacy policy and security practices of their smart devices, but label information from their previous study can convey risk to participants. Manikonda et al. [14] found smart speaker users’ type of concerning by analyzing 35.6M online review and custom study of 51 ASU student users. There were mainly 7 type of concerns - hacking device, collecting personal information, recording, listening 24/7, respecting user’s privacy, data storage repository, and creepy nature that it can be used as evidence in specific cases. Cho et al. [15] did a user study with 90 participants asking about customizing setting or content would affect their trust, credibility, security, and usability. By the survey, they found that manufacturers should consider incorporating various content customization options to lower users’ mistrust in content and relieve their concerns.

2.3.1 VPA in Multi-user Environment

Zeng et al. [19] have studied about fine grained access control and seamless authentication mechanisms in multi-user environments such as access control preferences, managing tensions, and conflicts between users. According to their research, they identified the challenges related to multi-user accounts for example, role of smart phone, auto login to primary account, authentication with regards to the environment and lack of flexible access controls. This paper suggests smart home access control and authentication systems should
be flexible enough to support a wide variety of use cases, people and types of relationships that exist in the home. Also, users need different types of access control in terms of people in their own house with role-based, location-based, and voice-based. Huang et al. [21] studied that there is a significant imbalance between users if there are multiple users in one house. According to the research, the participants experienced unauthorized voice purchases or unauthorized access to calendars and reminders, overheard call conversations and misuse of the device by unintended users like young children. They were also concerned on that their life pattern could be stored and sold to third parties or their conversations can be recorded. So, the authors in [21] concluded that the increased trust between smart speaker manufactures and the customers would increase adaptability of smart speakers. Also, the smart speaker should allow users to personalize their sharing preferences and the voice recognition technology should be improved to reduce the false positives. Geeng et al. [22] conducted mixed-methods qualitative study of interactions and tensions that occur between people sharing a smart home. They have combined semi-structured interviews with 18 participants that shares device with the others and experience sampling. There were two groups of participants, the people who instigate using smart home technology and who are less involved in smart home decision making. They researched concern of malfunction of Smart home technologies or when the network is down. They also found there is a slight difference of majority user between gender. On their research, male interviewees have participated more than female interviewee. This paper suggests the smart device manufacturers should design these devices easy-to-use mechanical switches and controls at least for basic features and considering different accounts for different users in the same household for various tasks.

2.4 Developers of VPA

The importance of detecting problematic application to prevent security problems and to keep consumers trust against service provider can be examined by the previous
research on similar platform, e.g. mobile device application market. Even though the mobile application market is bigger and lasted longer than the VPA market, they still have problems with privacy policies. On the previous research, Yu et al. [6] generated a module to analyze the privacy policies from the mobile market. By using their module, they could detect 23.6% of popular application has incomplete privacy policy. Zimmeck et al. [7] also generated automated large-scale machine learning analysis of privacy policies to pick out the application that is inconsistent. These study’s purpose is to make sure all applications to have adequate privacy policy to avoid security issues and to maintain high reliability of mobile markets. From those problems from similar platform market, we can expect the security problems that could be caused on VPA platform market if there is a lack of required privacy policies of skill in the market. Lots of previous research have tried to make an effective detection model to detect an application that has broken privacy policies.

The fundamental reason for so many problematic skills is that even some developers do not know much about requirements for voice-apps. For example, Le et al. [32] has studied about the risky skills in Kid’s category on Amazon Alexa market. They built a system to interact with the skills to uncover risky content for children. By using that, they found skills with inappropriate content for children, or skills that collects personal information. Also, they conducted a user survey of parents and found that many of them are not aware of parental control feature, so a lot of children are exposed to risky skills. Song et al. [4] conducted a comprehensive analysis on privacy policy on two major platform. By analyzing it, they found that a substantial number of problematic privacy policies exist on those platforms. For Amazon Alexa, they allows multiple voice-apps to have same invocation phrase, that make users risky to activate a voice-app that has problematic privacy policy [40]. From the result, they showed even VPA device’s own official voice-apps violates their requirements.
2.5 Social Bias of Smart Speaker

Koenecke et al. [26] investigated age and gender can impact the performance of Automatic Speech Recognition systems by conducting an interview with 42 white speakers and 73 black speakers and matching to select a subset of audio snippets of white and black speakers. Liu et al. [24] studied fairness on dialogue systems with several factors as gender or race. They used politeness, diversity, sentiment, and attribute words for their measurements and by training dialogue model for their experiment, they found that there are significant gender and race biases in dialogue system. Martin et al. [25] investigated the affects on habitual “be” in automated speech recognition by training ASR models with audio data. They found that the result of speech recognition can vary with people’s talking habit by showing habitual “be” has more error prone than non-habitual “be”, but acoustic factors don’t have big consistent effect.

2.6 Focused Problems

Figure 2.2 shows the concept of problems this paper would focus. The VPA device usually direct users to market’s web page with other mobile device so consumers can read voice-app’s privacy policy and the data type that voice-app is collecting. But there’s a lot of voice-apps that have problematic privacy policy documents. The needs of user’s perception on privacy policy arose here. Also, on the voice-app market side, there are a lot of content restrictions and privacy policy requirements, we wanted to know user’s awareness on policy requirements. The VPA device can be connected with various other smart devices and used by multiple users. It understands consumer’s command with ASR and NLU, but those techniques are not perfect and have weak authentication than user expects, and as voice-app markets allows to have same or similar invocation phrase, user can activate different voice-app that can be malicious. Also, their speech recognition has accuracy bias between gender and age, etc. So we wanted to know user’s concern on multiple user environment and to collect user’s perception on social bias. The voice-app market allows third-party developers
to submit their voice-app. Although they have their own policy requirements and voice-app certification process, developers can change their back-end code after approval, which makes the whole process untrustworthy. Also there are a lot of conditions for developers to check, we wanted to figure out the fundamental reasons for problematic voice-apps.

Figure 2.2: Problem Highlight
Chapter 3

Methods

3.1 Recruitment

We created our survey and collected data via online survey platform ‘Qualtrics’, which allows researchers to create a survey and simply superintend it such as skip logic, display logic with survey flow. Also, we recruited 60 users for each survey except developers (30 participants) with separate recruitment batch, using Amazon Mechanical Turk (MTurk) platform. All survey questions are listed in the appendix. To conduct a fairness survey, we recruited trustworthy MTurk users who currently lives in United States and have Human Intelligence Tasks (HITs) approved at least 500 prior this study. Each participants received $1 for their participation with the code provided at the end of survey.

All participants for each survey were asked for few screening questions to filter out Clemson University’s faculty or student, participant that didn’t used or owned smart speaker, and the person who have short experience with their smart speaker (less than one month). For the developer’s part, we collected 30 participant’s responses. To ensure collecting appropriate responses, the participants for this survey had to take some screening questions to filter out real-experienced voice-app developers. We first asked whether they have developed any Alexa skill or Google Action, and what platform’s voice-app they developed so we can compare their response for the next question. Then we asked them to
list two default intents when you create a new skill or action, which all voice-app developers should be familiar of. This was a process to ensure selected participants have enough personal experience with their smart speaker. The filtered participants cannot start the main survey questions so they cannot have access to the code given at the end of survey. The study was reviewed and approved by Clemson University IRB office.

3.2 Purpose of the Study

3.2.1 User’s Engagement with Privacy Policy

Smart speakers are much easier to access whether of ages than other devices, but unfortunately, smart speakers’ voice-apps are hard to check its policies for users due to lack of display panels. For the user, if they want to know the skill has adequate policy, it could be checked with other devices such as mobile phone. The VPA voice-app market allows third-party developers to submit their voice-apps, but the VPA voice-app market does not check the existence of a proper privacy policy or do not make it essential by developers to submit their voice-app. Also, the voice-app’s back-end code can be changed by the developer after being published on the market, which can allow change of collected data type of voice-app may against the initial privacy policies that were originally adequate. Those gaps allow skills to have a lack of privacy policies or having wrong privacy policies for the skill. Consumers would be frustrated when they face the voice-app that has wrong or lack of privacy policy. So, we want to encounter about users’ experiences, perspectives, concerns, and how users engage with privacy policies of voice applications on VPA devices.

3.2.2 Awareness of Different Policy Requirements

As mentioned previously, there are more than one voice assistant platform / market and each of them has unique privacy policy requirements and restrictions. Also, the markets have different policies between categories of voice-app. Because of the diversity of policies, understanding whether users and developers are aware of various policy require-
ments including sharing user information with third parties defined by VPA platforms is needed.

3.2.3 User’s Concerns in Multi-User Environment

Unlike mobile phone’s VPA service, the smart speaker can be accessed with multiple users. The smart speakers are usually used in a house, and there is a lot of types of house members these days. The users could be a family consisting of adults or with kids, guests, housemates(roommates), and more. There could be a security problem and complaints because of this diversity, such as concern about unauthorized access by impersonate to calendars and reminders [21]. So the need for a fine-grained multi-user access control for smart speaker users has appeared. We created a survey block for each type and asked participants about their circumstances - how many people uses their smart speaker, whether they use it as smart home controller and who does uses it. By the participant’s selection, they can be directed to the appropriate survey blocks based on their multi-user circumstance.

3.2.3.1 Examples of Multi-User Environment

There could be several types of multi-users in VPA devices. The most common type would be family, but there could be other types of residence and there could be issues between those multiple users. This paper classified the types of residence into four types including smart home controller as a multi-user environment.

1. Parent-children: The smart speaker is very easy to access, but it’s unfriendly for parent consumers. The VPA device has weak voice authentication, it’s common for consumer to face executing the wrong voice-app while using the VPA device. Sometimes those wrong voice-app contains violence content, it could be risky if there is child listening. There are a lot of contents that has similar names and smart speakers can make mistakes with their commands in VPA market. A lot of children treat the smart speaker as their playmate and ask them various questions or commands. Due to child’s pronunciation, it is not difficult for children to execute the very wrong voice-
app that contains risky contents for them. Also, the smart speakers could be linked to personal accounts for consumers’ convenience, but it has low authentication for using the account, child could accidentally order things or send a personal information that their parents don’t aware of [39].

2. **Guest**: The smart speakers could be linked to personal accounts of original user, so the user can easily access to their account and order something or check their schedule or search for items they want. But it could be abused by strangers - the smart speaker can activate with anybody’s voice. There could be a guest that are not friend of the owner of smart speakers, such as construction worker or delivery driver, it is possible they can accidentally encounter privacy issues.

3. **Roommate**: There could be someone who lives with their roommates (which is not their family) for various reasons. The smart speakers do not have strong speaker recognition, which can make privacy problems such as accessing contact list or calendar events.

4. **Smart Home**: Due to rapid increase on smart home devices, a lot of users are using their smart speakers as their smart home controller. Smart home devices are directly linked to user’s security, but smart speakers can activate and used by anyone. Even a little problem caused by smart speaker, it could be critical security problem such as unlocking all doorways by accident.

### 3.2.4 Developer’s Perception of General Policies

The developer must consider more features and has a different perspective compared to general users. They must know the requirements of each platform and meet those requirements. For example, on Alexa market, collecting kids or health data violates their policy. For general categories, the application cannot ask customers for positive rating, cannot include toxic content, and cannot predict the gender of user. But as shown in the previous studies [32, 4], there are a lot of problematic voice-apps that violates restricted content
requirements and privacy policy requirements. This might because of various policy with each manufacture’s market and have different policies with categories, it is hard to expect all developers are aware of it and they always meet the conditions. So, we wanted to find out the fundamental reason how these problematic voice-apps could exist.

3.2.5 Social Biases of Speech Recognition

Human voice data includes a lot of information of characteristics such as anatomy and learned behavioral patterns (acoustic patterns) that make available use as specific personal identification. By analyzing the voice, people can expect voice owner’s gender, age, and race. However, unlike human, VPA device’s ASR and NLU is not accurate or flexible, it can occur misunderstanding on consumer’s command. Because of that, there are social biases on VPA services but not a lot of users are not aware about it. The results could be differed by gender, race, and age with same command. These gaps may continue and worsen existing inequalities against minority group problems in a multi-user environment. So, we wanted to get user experiences and perceptions of social biases of speaker recognition and speech recognition in smart speakers.
Chapter 4

Results and Findings

On the survey, the 70% of participants were using Amazon Alexa and 30% of participants were using Google Echo.

4.1 General Usage

For all surveys, the main purpose of using smart speaker was for voice assistant (69%), as a bluetooth speaker (17%), as for smart home controller (14%). Only 5% of participants answered as they did not linked their accounts to the smart speaker.

4.2 Both VPA User’s and Developer’s Issue

4.2.1 Awareness of Policies

*Awareness of different policy restriction and privacy policy requirement.* From the survey, we could get 60 participant’s responses. Most of users are aware of policy restriction differences between categories, but a lot of users experienced violence of the restrictions. 74% responded they know that each category on the market has different policy restrictions. But a lot of user experienced applications violating their platform’s general policy requirements such as privacy policy. 80% of user experienced that their device collecting their health
data when they were using a health category’s voice-app, and 42 out of 60 participants have experienced that their device didn’t show them privacy policy even their voice-app was trying to collect their personal data.

**Awareness on data usage.** Most of participants were aware of data types that are collected and data sharing with third parties. When we asked users know what data type their device collects for using voice-app, only about 17% responded they are not aware about the data type. But half of users are not aware that third parties could share their data while using the voice application. Figure 4.1 shows the scale ratio of ‘always listening’ feature and third-party data sharing. 42% felt uncomfortable with third parties collecting their data. The most preferred term for their data storage on third-party was for 6 months to 12 months. 17% expected less than 6 months, 47% expected between 6 months to 1 year, 18% expected more than 2 years. Most users are aware of ‘Always listening’ concept of smart speaker, but about 27% were uncomfortable with that concept. This shows even though users are concerning about their privacy, most of them feel comfortable, which implies that consumers usually trust their device provider.

<table>
<thead>
<tr>
<th>Questions</th>
<th>Response</th>
<th>% of users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have you used more than one smart speaker?</td>
<td>Yes</td>
<td>73%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>27%</td>
</tr>
<tr>
<td>Did you experience that your device collecting your health data when you were using health application?</td>
<td>Yes</td>
<td>80%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>20%</td>
</tr>
<tr>
<td>Did you experience that your device didn’t show you privacy policy even your application was trying to collect your personal data?</td>
<td>Yes</td>
<td>70%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>30%</td>
</tr>
<tr>
<td>Do you know your data could be shared with the other third-parties like advertisers?</td>
<td>Yes</td>
<td>47%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>43%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>13%</td>
</tr>
<tr>
<td>Do you know what data type that your device collects for using skills?</td>
<td>Yes</td>
<td>83%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>17%</td>
</tr>
<tr>
<td>Do you know the concept of the smart speakers ‘always listening’?</td>
<td>Yes</td>
<td>95%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>5%</td>
</tr>
<tr>
<td>How long do you expect the third-party would store your data?</td>
<td>Less than 6 months</td>
<td>17%</td>
</tr>
<tr>
<td></td>
<td>6 - 12 months</td>
<td>47%</td>
</tr>
<tr>
<td></td>
<td>1 - 2 year</td>
<td>18%</td>
</tr>
<tr>
<td></td>
<td>More than 2 years</td>
<td>18%</td>
</tr>
</tbody>
</table>

Table 4.1: Awareness survey questions and % of responses
4.3 Issues Encountered by VPA Users

4.3.1 User’s Perspective on Privacy Policy

Users’ privacy concern. From the survey, we could get 60 participant’s responses. Table 4.2 shows the survey responses from smart speaker consumers. We could find that 64% of participants experienced activating unexpected voice-app, which shows it is common to invoke the other voice-app. Most of consumers use their voice to enable new voice-app. Although most of participants were satisfied with their experience on smart speaker, 54% of participants responded that they have concerns while using the smart speaker even though they adopted the smart speaker. 46% of participants tried to turn off their devices
over concerns of security. Their major concern was that someone can eavesdrop their daily conversation (56%) or leak of personal information (44%). For specific personal information concern, participants replied that the most concerned personal information is their security numbers like Social Security Number or their account information (75%), and address (12%), phone number (8%) followed that.

Users’ proficiency of device. Most of the users were skilled enough to use the device in-depth, but not a lot of them used those features. As you can see on the Table 4.2, when we asked about if they ever tried to disable the voice-app after using the specific voice-app, about 33% of users responded as they did. The main reason was to avoid security issues, some of them felt they had no need of the voice-app, or to avoid purchasing something by accident. However, some of consumers disabled voice-app to check how smart speaker works. More than half of participants were aware how to access to the logs or other debugging features. The reason of person who never check the logs or debugging features were because most of consumers thought they felt unnecessary to check it, but some of them couldn’t do it because they don’t know how to check it.

Users’ attitude on privacy policy. Most of users concern of their privacy and security, but there are a lot of users who do not read the privacy policy provided by developer. Figure 4.2 shows users’ perception of reading privacy policy, existence of privacy policy affects enabling voice-app and does a voice-app needs adequate privacy policy. A lot of users agreed with all voice-apps need adequate privacy policies, but about 25% replied they don’t read the privacy policy actually. But even they don’t read the policy, 43% of participants agreed the existence of policy affects to enabling the new voice-app. Since more than half of participants does not care about existence of privacy policy, this implies that a lot of users trust the smart speaker provider.

4.3.2 User’s Attitude Toward Multi-User Environment

Types of shared users. For this survey, we could get 60 participant’s responses. 73% replied more than 2 people use one smart speaker at their house, which implies multiple user
<table>
<thead>
<tr>
<th>Questions</th>
<th>Response</th>
<th>% of users</th>
</tr>
</thead>
<tbody>
<tr>
<td>How do you enable new skills?</td>
<td>By voice</td>
<td>69%</td>
</tr>
<tr>
<td></td>
<td>By mobile device</td>
<td>31%</td>
</tr>
<tr>
<td>Do you have experienced that different skill encountered rather than the skill you originally wanted?</td>
<td>Yes</td>
<td>64%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>36%</td>
</tr>
<tr>
<td>Did you try to turn off your device over concerns of security?</td>
<td>Yes</td>
<td>46%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>54%</td>
</tr>
<tr>
<td>Do you have concerns using your smart speaker?</td>
<td>Yes</td>
<td>54%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>46%</td>
</tr>
<tr>
<td>What's the major concerns with it?</td>
<td>Someone can eavesdrop my conversation</td>
<td>56%</td>
</tr>
<tr>
<td></td>
<td>Leak of my personal information</td>
<td>44%</td>
</tr>
<tr>
<td>Have you used your device to purchase something?</td>
<td>Yes</td>
<td>61%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>39%</td>
</tr>
<tr>
<td>Have you tried to disable the skill after using it?</td>
<td>Yes</td>
<td>33%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>67%</td>
</tr>
<tr>
<td>Have you accessed device logs or other maintenance or debugging information of your device?</td>
<td>Yes</td>
<td>58%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>42%</td>
</tr>
<tr>
<td>Have you experienced trouble with stolen privacy policy?</td>
<td>Yes</td>
<td>38%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>62%</td>
</tr>
<tr>
<td>What personal information security concerns you the most?</td>
<td>Address</td>
<td>13%</td>
</tr>
<tr>
<td></td>
<td>Birth date</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>Security Numbers</td>
<td>73%</td>
</tr>
<tr>
<td></td>
<td>(SSN, account info, etc.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone number</td>
<td>9%</td>
</tr>
<tr>
<td>Have you ever provided your personal information to your device by speaking to it?</td>
<td>Yes</td>
<td>45%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>55%</td>
</tr>
</tbody>
</table>

Table 4.2: Privacy policy survey questions and % of responses

access is not uncommon. Most of users were sharing their device with their family. 50% of them were sharing the device with their spouse, 37% were sharing with their children, 13% of them were sharing with their parents. All of the participants were using their smart speaker as a smart home controller also.

Smart home controller usage. A lot of participants were using more than 1 smart home devices. 40% of participants were using the smart speaker to control one to two devices, 46% were using it to control three to four devices. Although they use it as a smart home controller, we could find that a lot of users do not know that they can limit device access. 10% replied some of their non-primary users (households) cannot control access to
smart home devices, and 10% replied that they cannot limit their device access for their smart home. The major concern using as smart home controller was security and privacy. When we asked about what kind of security policies they would like to have or expect for their smart speaker as smart home controller, the participants replied as to have high security of passwords and having limited access, or age restriction, such as guest or kids’ mode that allows easy and quick switching feature. Even they are using their device as smart home controller, few users experienced someone else using their device to control their smart devices.

*Guest situation.* Most of users change their usage of VPA device while someone
that is not their household (including stranger and friends) stays in their house. Figure 4.3 shows the ratio of consumers’ comfortableness on guests using VPA device, only about 34% of participants were uncomfortable with guest using. Also, on Figure 4.4, it shows that 21% of participants does not agree with the fact that stranger can access their personal information. When we asked them does your usage change if there are others who are not your family, 43% replied it does not change. About half of consumer replied that their guests never have used or tried to use their smart speaker, but more than half of participant replied they would or might turn off their device when someone comes to their home. Also 50% responded that they change settings of their speaker to protect privacy when someone is expected to come over their home. Users could be affected with their guest’s experience while using their device. Although 32% responded that their guest tried to tell their personal information to the device while using it, 78% of them replied it effected the later use of the same voice-app and 78% of them deleted the voice-app because of it.

*Parent-children situation.* A lot of participants don’t let their children to enable a voice-app of smart speaker but by contrastively, most of participants were not uncomfortable to let their children using the device alone (Figure 4.5). For the users who have children in their house, about 75% had kids under 13. 60% of parent user responded as they check
privacy polices of kid’s voice-apps before enabling for their children. Most of parent users don’t let their children to enable new voice-apps without asking for their permission, but only 20% of parent users responded that they feel uncomfortable when kids saying personal information to VPA device. Not a lot of parent users are concerned about the children’s usage although the misunderstanding of command is common. 45% checks the log after their kid using the smart speaker. 25% experienced to get a violent or sexual content response, which can be risky for children. Most of participants limit those problems by disabling the voice-apps, but 25% limits it by muting the device when kids are with the device, 25% limits
by not letting kids using the device. Also, 55% replied they would limit their use of the smart devices in front of children if their children are young, but 45% replied their usage does not change even if they are with their kids. Only 5% replied they never experienced with their device misunderstands them or their children’s commend and replied to different command, and 40% replied it was children’s command, 20% replied children and adult’s rate was similar.

Figure 4.5: User’s scaled perception on parent-kids environment

Unfortunately, there were too small amount of roommate residential type (2 responds) and they had same positive responds, we couldn’t get reliable results for user’s privacy concern on roommate side.
For multiple user circumstances, user asked to have easy changing mode feature for guests and children, or specific voice recognition so only verified user’s command could activate the device. By this result, we could find that even the VPA device manufacturer provides speaker recognition, a lot of consumers are not aware of that feature. Also, VPA device provider should make easy-quick change mode for guest and kids so user can easily limit the access in various circumstances.

4.4 Issues with VPA Developers

4.4.1 Developer’s Perception of Policy Requirements and Privacy Policy

*Difficulty with policy requirements.* By those screening questions, we could filter out 10 real voice-app developers. We could collect 9 Amazon Alexa developer and 1 Google Assistant developer. Even though most of them were Amazon platform developer, when we asked how does their device’s market check and test their voice-app, 5 responded that their device’s market checks before published and the other 5 responded that it checks after published. Also, for the question how do you get noticed or checked with platform’s required privacy policy rules, 5 of them replied by notification of platform also 5 of them replied they check it by searching manually. Also, for checking the privacy policy and restriction requirement, most of developers responded they usually check their code manually by comparing their voice-app’s stored information and the platform’s requirements. There was a participant who replied as he copies the same category’s voice-app.

*Attitude toward the privacy policy and policy restrictions.* Most of participants complained the difficulty to generate an adequate privacy policy for their voice-app. For the question about how they generate a privacy policy, they replied as search for a policy provider, some search the way to generate privacy policy that meets requirements of the platform, and some generate it by analyzing their application with which collects what types of data and protocol. All participants responded as they provide adequate privacy policy for users. Surprisingly, although they replied they provide valid privacy policy for users, they have ex-
periences to copy the privacy policy. 30% of them have an experience to copy privacy policies from the other voice-apps (including their own voice-apps). Conspicuously, as shown on Figure 4.6, one participant disagreed that an appropriate privacy policy is necessary for the voice-apps that collects user’s data because he personally don’t care about the existence, while most of developer participants agreed with it. Developers were aware of the importance of an appropriate privacy policy. As shown on Figure 4.7, all participants replied as an adequate privacy policy impacts their voice-app rate, 90% of participants replied as privacy policy have an important role for their voice-app. A lot of developers think the most important role of privacy policy is to make their voice-app dependable for users, 30% of developer participants replied that it is commitment for end users. most of participants were aware of privacy policy requirements and general policy restriction requirements on their platform market, but most of them had an experience to violate those policy requirements.

![Figure 4.6: Developers’ scaled perspective on privacy policy](image)

For the privacy policy, most of developers are aware if they collect personal data from end users, they must provide and display a legally adequate privacy policy about the applications’ collecting data within the app and on the detail page. But as mentioned previously, they have to search the way to generate it or copy the existing privacy policy for their ease. On Figure 4.8, 90% of developer participants feels importance of privacy policy generating program. For the general policy requirements, 60% of participants were aware
that they cannot ask customers for positive rating. But 8 participants replied they have added a feature to ask their customers for positive rating, including 4 participants who were aware that it violates platform’s policy restriction. The biggest reason was to improve feature with it or just it helps their voice-app. Also, most of developers are aware of their platform’s general policy restrictions, such as each child or health category policies of their market and cannot contain toxic or inappropriate content. But although they are aware of the policy restrictions, a lot of developers do not meet the condition for their benefits. 50% of participants have promoted any products, content, services that directs end users to engage with content outside of Alexa in Kids category voice-app even 80% of them knew that violates policy of Alexa. Also, most of developers are aware that health application cannot provide health-related information or tips and does not include a disclaimer in the voice-app description is violating the policy of Alexa. By analyzing the results, we could find that even though the platform made policy restrictions and privacy policy requirements, they do not check applications on their market meticulously and frequently before publishing or after publishing the voice-app. Because of that, it is possible for developers to publish a problematic voice-app that violates the privacy privacy requirement and also general content requirements. This shows how developers think and how they treat their voice-app’s requirements.
4.5 VPA System Issue

4.5.1 Fairness on VPA Devices

Users’ perception of social bias on Smart speaker. For this survey, we could collect 60 participant’s responses. The participant’s age was ranged from 16 to 65 years old. When we asked them to have you ever noticed that the device understands other people’s commands better than your own while using the smart speaker, 38% responded as ‘yes’. About 33% replied as smart assistants better understood anyone of a different gender than them, the male’s response ration was bigger than females. This supports the previous study of Feng et al. [23]. 27% replied as it better understood anyone of different race, and the participant’s race were mostly White due to the high proportion of white people among participants, but there were also Black or African American, American Indian, Asian responses. 30% replied as it understood better with a person of a different dialect, and 35% replied as it understood better with a person of a different age. By the later question, we could find those understanding difference between age occurs dissatisfy for parent user due to their concern with children use experience. 15% replied they think their smart devices has a bias with understanding commands within their households, also 30% replied it might have a bias. For their and their households’ experience, 1 - 5 times of misunderstanding command
was common with 68%, but 17% answered as they have experienced more than 10 times. The participants answered when it starts to misunderstand their command, it takes a long time to make their smart device to understand the correct command, which makes them feel frustrated and wasting their time. 58% answered as they experienced problems with misunderstanding command issues. Most of participants answered everyone in their house have the same level of access (87%). Interestingly, 62% replied they have to change the way to talk to be understood by their smart speaker. For example, changing the speed of their chat like talking slowly or talk in a high volume. 28% of participants responded as they personally had some problem within misunderstanding issues. One participant specified their problem, they have set a timer and alarm by their smart speaker but it set the timer / alarm on different time, so they had trouble with their schedule.

4.6 Limitations

On this survey, we collected limited amount (less than 100) of responses for each survey. On Multi-user part, we collected multiple resident type responses on one survey for multi-user environment part, so we had very few responses (2 response) for roommate circumstances. Since roommate residential type is very common in big cities, the user experience on roommate scenario could be conducted with large comparison group. On developer’s survey, after the screening question filtering, we could get small amount of reliable responses, smaller than expected. For the further study, there should be more researches on developer’s perception of voice-app developing. Also, on the fairness survey, White people had high proportion among the participants. Over 80% were White, so we couldn’t collect enough user’s experiences of users of various races. As the smart speaker sales market is expected to expand, the service provider should be well prepared for global users. Also, we focused only on NLU to get users perception of social bias because our user study was conducted for normal users that are not technical. But also NLP (Natural Language Process) can cause social bias, there should have user study for NLP side.
Overall, the number of participants in this user study is not enough big to normalize the user’s experience, there could be a survey with more participants. Also, we only collected specific text entry responses for negative responses, for further study, they should also gather specific reasons for positive responses.
<table>
<thead>
<tr>
<th>Questions</th>
<th>Response</th>
<th>% of users</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many people in your house use the device?</td>
<td>1</td>
<td>27%</td>
</tr>
<tr>
<td></td>
<td>More than 2</td>
<td>73%</td>
</tr>
<tr>
<td>Except you, who else uses smart speaker?(multiple choices)</td>
<td>Parents</td>
<td>13%</td>
</tr>
<tr>
<td></td>
<td>Spouse</td>
<td>50%</td>
</tr>
<tr>
<td></td>
<td>Kids</td>
<td>37%</td>
</tr>
<tr>
<td></td>
<td>Siblings</td>
<td>2%</td>
</tr>
<tr>
<td></td>
<td>Roommates</td>
<td>3%</td>
</tr>
<tr>
<td>Do you use your smart speaker as a controller of smart home?</td>
<td>Yes</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>0%</td>
</tr>
<tr>
<td>When there are others – that are not your family – around you, does your usage change with the smart speaker?</td>
<td>Yes</td>
<td>32%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>43%</td>
</tr>
<tr>
<td>Does your guest use your smart speaker? Or was there anyone who tried to use it?</td>
<td>Yes</td>
<td>23%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>30%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>47%</td>
</tr>
<tr>
<td>Do you make your smart speaker turn offed when someone comes to your home?</td>
<td>Yes</td>
<td>40%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>45%</td>
</tr>
<tr>
<td>Do you change settings of your speaker to protect your privacy when someone is expected to come your home?</td>
<td>Yes</td>
<td>50%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>50%</td>
</tr>
<tr>
<td>Did one of your guests tried to tell their personal information to your device?</td>
<td>Yes</td>
<td>28%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>72%</td>
</tr>
<tr>
<td>Did it effect your later use of same skill/ability?</td>
<td>Yes</td>
<td>76%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>24%</td>
</tr>
<tr>
<td>Did you deleted the skill/ability because of it after when they are gone?</td>
<td>Yes</td>
<td>60%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>31%</td>
</tr>
<tr>
<td>How many devices can you control with your smart speaker?</td>
<td>1 - 2 devices</td>
<td>40%</td>
</tr>
<tr>
<td></td>
<td>3 - 4 devices</td>
<td>46%</td>
</tr>
<tr>
<td></td>
<td>More than 4 devices</td>
<td>14%</td>
</tr>
<tr>
<td>Is everyone in your house accessible to smart home?</td>
<td>Yes</td>
<td>77%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>13%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>10%</td>
</tr>
<tr>
<td>Can you limit your device access for your smart home?</td>
<td>Yes</td>
<td>50%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>31%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>19%</td>
</tr>
<tr>
<td>Do you have concern while using it?</td>
<td>Yes</td>
<td>48%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>52%</td>
</tr>
<tr>
<td>Have you ever had arguing with people in your home about using smart home?</td>
<td>Yes</td>
<td>30%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>70%</td>
</tr>
<tr>
<td>Did you have an experience that your guest using your device as a smart home controller?</td>
<td>Yes</td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>23%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>57%</td>
</tr>
<tr>
<td>Do you have kids under the age 13 who uses the device?</td>
<td>Yes</td>
<td>75%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>25%</td>
</tr>
<tr>
<td>Do you check the privacy policies before using the skills for your children?</td>
<td>Yes</td>
<td>60%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>40%</td>
</tr>
</tbody>
</table>
### Table 4.3: Multi-user survey questions and % of responses

<table>
<thead>
<tr>
<th>Questions</th>
<th>Response</th>
<th>% of users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you let your children to download voice assistant applications without asking?</td>
<td>Yes</td>
<td>35%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>45%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>20%</td>
</tr>
<tr>
<td>Do you check the log after your kid using it?</td>
<td>Yes</td>
<td>45%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>55%</td>
</tr>
<tr>
<td>Do you experienced to get a violent/sexual content response from your device? (Not good for kids)</td>
<td>Yes</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>75%</td>
</tr>
<tr>
<td>How do you limit those problems?</td>
<td>By muting the device when kids are with the device</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>By not letting kids using the device</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>By disabling the skills</td>
<td>50%</td>
</tr>
<tr>
<td>Do you have kids under the age 13 who uses the device?</td>
<td>Yes</td>
<td>75%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>25%</td>
</tr>
<tr>
<td>If your children are young, do you limit to use the smart devices in front of them?</td>
<td>Yes</td>
<td>55%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>45%</td>
</tr>
<tr>
<td>Is there difference of usage when if you are with your kids, and if you are with adults or alone?</td>
<td>Yes</td>
<td>40%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>60%</td>
</tr>
<tr>
<td></td>
<td>Never did</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>1 - 3 times</td>
<td>35%</td>
</tr>
<tr>
<td></td>
<td>3 - 5 times</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>5 - 10 times</td>
<td>25%</td>
</tr>
<tr>
<td></td>
<td>More than 10 times</td>
<td>25%</td>
</tr>
<tr>
<td>How many times did your device misunderstood you/your children’s command and replied different command?</td>
<td>Parent</td>
<td>40%</td>
</tr>
<tr>
<td></td>
<td>Children</td>
<td>40%</td>
</tr>
<tr>
<td></td>
<td>Similar rate</td>
<td>20%</td>
</tr>
<tr>
<td>Questions</td>
<td>Response</td>
<td>% of users</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>How does your device’s markets check and test your skills?</td>
<td>Before published 50%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>After published 50%</td>
<td></td>
</tr>
<tr>
<td>Are you aware of required rules of policies of VPA platform?</td>
<td>Yes 100%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No 0%</td>
<td></td>
</tr>
<tr>
<td>How do you get noticed or get checked with those required rules?</td>
<td>By searching 50%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By notification of platform 50%</td>
<td></td>
</tr>
<tr>
<td>Do you think an appropriate privacy policy is necessary for skills that</td>
<td>Yes 90%</td>
<td></td>
</tr>
<tr>
<td>collect user’s data?</td>
<td>No 10%</td>
<td></td>
</tr>
<tr>
<td>Do you provide valid privacy policy for your skill?</td>
<td>Yes 100%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No 0%</td>
<td></td>
</tr>
<tr>
<td>Have you copied privacy policies from the other skills?</td>
<td>Yes 30%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maybe 40%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No 30%</td>
<td></td>
</tr>
<tr>
<td>What do you think the most important role of privacy policy?</td>
<td>Confidence for the skill 70%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Commitment for end users 30%</td>
<td></td>
</tr>
<tr>
<td>Do you know you cannot ask customers for positive rating?</td>
<td>Yes 60%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No 40%</td>
<td></td>
</tr>
<tr>
<td>Have you added a feature to ask your customers for positive rating?</td>
<td>Yes 80%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No 20%</td>
<td></td>
</tr>
<tr>
<td>Are you aware of Kids/Health category’s policies of your market?</td>
<td>Yes 80%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No 20%</td>
<td></td>
</tr>
<tr>
<td>Are you aware that for Kids/Health category cannot contain</td>
<td>Yes 70%</td>
<td></td>
</tr>
<tr>
<td>toxic/inappropriate content?</td>
<td>No 30%</td>
<td></td>
</tr>
<tr>
<td>Have you promoted any products, content, services that directs end users</td>
<td>Yes 50%</td>
<td></td>
</tr>
<tr>
<td>to engage with content outside of Alexa in Kids category skill?</td>
<td>No 50%</td>
<td></td>
</tr>
<tr>
<td>Did you know that violates policy of Alexa?</td>
<td>Yes 80%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No 20%</td>
<td></td>
</tr>
<tr>
<td>Are you aware that a Health application cannot provide health-related</td>
<td>Yes 60%</td>
<td></td>
</tr>
<tr>
<td>information or tips and does not include a disclaimer in the skill</td>
<td>No 40%</td>
<td></td>
</tr>
<tr>
<td>description is violating the policy of Alexa?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you aware you must provide and display a legally adequate privacy</td>
<td>Yes 70%</td>
<td></td>
</tr>
<tr>
<td>policy about the application collects what kind of personal data from</td>
<td>No 30%</td>
<td></td>
</tr>
<tr>
<td>end users within the app and on the detail page?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you always provide adequate privacy policy for each or your</td>
<td>Yes 100%</td>
<td></td>
</tr>
<tr>
<td>application?</td>
<td>No 0%</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.4: Developer survey questions and % of responses
<table>
<thead>
<tr>
<th>Questions</th>
<th>Response</th>
<th>% of users</th>
</tr>
</thead>
<tbody>
<tr>
<td>While using a smart speaker, have you ever noticed that the device understands other people’s commands better than your own?</td>
<td>Yes</td>
<td>38%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>62%</td>
</tr>
<tr>
<td>Have you ever had a smart assistant better understand anyone of a different gender than you?</td>
<td>Yes</td>
<td>33%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>67%</td>
</tr>
<tr>
<td>Have you ever had a smart assistant better understand anyone of a different race than you?</td>
<td>Yes</td>
<td>27%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>73%</td>
</tr>
<tr>
<td>Have you ever had a smart assistant better understand anyone of a different dialect than yours?</td>
<td>Yes</td>
<td>30%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>70%</td>
</tr>
<tr>
<td>Have you ever had a smart assistant better understand anyone of a different age than you?</td>
<td>Yes</td>
<td>35%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>65%</td>
</tr>
<tr>
<td>Do you think your smart device have a bias with understanding commands within your households?</td>
<td>Yes</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>Maybe</td>
<td>30%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>55%</td>
</tr>
<tr>
<td>How many times does it misunderstand your/household’s command?</td>
<td>1 - 5 times</td>
<td>68%</td>
</tr>
<tr>
<td></td>
<td>6 - 10 times</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>More than 10 times</td>
<td>17%</td>
</tr>
<tr>
<td>Did you experienced problems with misunderstanding command?</td>
<td>Yes</td>
<td>58%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>42%</td>
</tr>
<tr>
<td>Does everyone in your household have the same level of access?</td>
<td>Yes</td>
<td>87%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>13%</td>
</tr>
<tr>
<td>Do you have to change the way you talk to be understood by your smart speaker?</td>
<td>Yes</td>
<td>62%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>37%</td>
</tr>
<tr>
<td>Have you or anyone you know ever been personally affected due to a misunderstanding by your smart speaker?</td>
<td>Yes</td>
<td>28%</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>72%</td>
</tr>
</tbody>
</table>

Table 4.5: Fairness survey questions and % of responses
Chapter 5

Discussion and Conclusion

5.1 Discussion

Smart speaker is very fascinating device that is expected to provide a lot of benefits for customers. They offer to control other smart home devices and to control users’ lifestyle with it. Although previous studies have examined about users’ privacy concern and multi-user situation issues, there has been a few research on users’ perceptions of social bias on smart speaker and concerns on both customers and developers.

While doing the survey, we could find out that most of users trust the VPA device provider company, so more than half of them don’t feel uncomfortable with the fact their data can be shared with third-party. Also among the consumers, only a few of them feel uncomfortable with always listening features although it could cause privacy problem. Although users mostly trust on VPA device provider, the device’s misunderstanding command is common. The VPA device should improve their speech recognition to maintain user trust. As the previous study [4, 41, 10], the ratio of valid privacy policy is very low and attackers can make similar name by paraphrasing, wrong speech recognition will allow user to encounter wrong voice-app that can cause security problems.

Most of users link their account to smart speaker for their convenient use, but because it can be used by multiple people, it should have easy feature to change the user’s account.
From the survey, we could find that a lot of users (14 of 25 users) expect at least two other modes – guest mode and kids’ mode. Since users experienced with their VPA device about misunderstanding command issue and poor authorization on shopping, they expect to have a change mode for guest and children. Those mode can be used when guest comes over or their children uses the device without guardian. For example, on the guest mode people can ask for general questions like asking weather but enabling new voice-app or buying something should be limited. For the kid’s mode, user can only use kids’ category voice-app with basic features that device provides such as searching questions. Or simply, if user changes mode, all linked account becomes disable for security. The VPA device provider should promote about the speaker recognition function and how to use it. Surprisingly, although Amazon and Google provide specific speaker recognition, all of participants were unaware of these features. In the survey, consumers complained about the lack of speaker recognition.

Even though the VPA device market has privacy policy and policy restriction requirements, the platforms do not have strong sanctions to developers before publishing the voice-app and also do not check the lack of policies on the published voice-app frequently. This could lower consumer’s trust against the VPA device service provider.

For the social bias on VPA device, 23 out of 60 consumers have perception that smart speaker has social bias on age, gender, race, etc. When the device doesn’t understand the command of user, it usually doesn’t understand even very basic command like turning off or turning on the linked smart home device. There was a participant who even experienced that alarm/timer has set to different time so that participant had trouble with their schedule. The biggest complaint from the consumers was when the VPA device starts to misunderstand users command, they have to repeat it a lot which makes them to waste time, feeling stressed and frustrating with using their device. Sometimes they give up asking their device to doing something and search it with another device such as mobile phone or computer. Also with the same reason, it makes very hard for children to use smart speaker due to the situation.

Overall, most of the complaints are due to the VPA device company’s untrustworthy certification process. So the VPA device provider should impose stern rules in terms of the
skills used and make sure that their market’s voice-app abide by the privacy policies.

5.2 Conclusion

In this work, we have conducted 5 categories of surveys to understand users’ perceptions and developers’ perceptions of Voice Personal Assistants. We have collected a total of 250 responses from smart speaker users, including 10 voice-app developers. With the responses, we have discussed expectations of VPA device features on consumers and the strategies to keep trust from consumers to help VPA device providers figure out the gap between user’s expectations and to enhance their certification process.

For the future works, the biggest concern from the VPA device consumer is privacy and security. As there exists happening using wrong speech recognition, improving the design of speech recognition would be recommended for the future research. As mentioned on the consumer’s expectation on multi-user environment, design that provides quick and easy switch for various mode would be recommended for the future research.

The VPA devices provide speaker recognition to listen specific user’s voice command currently and user can block the voice-app or contacts for their preference. But it does not provide to block specific user’s voice command. Designing speaker recognition to block features for specific user would be recommended as the future research. This could help to increase consumers’ confidence about the child’s usage of the device without guardians.
Appendices
Appendix A  List of Survey Questions

The itemize of Survey Questions except screening Clemson University’s student or employee or their family members. The same general question would be omitted.

A.1 Privacy Policy

1. Do you use smart speakers, e.g., Amazon Alexa or Google Assistant?
   • Yes
   • No

2. How long have you been using the device?
   • Less than 1 months
   • 1 - 6 months
   • 6 - 12 months
   • 1 - 2 years
   • More than 2 years

3. What is your gender?
   • Male
   • Female
   • Non-binary / third gender
   • Prefer not to say

4. What age group are you?
   • Under 18
   • 18 - 25
   • 26 - 45
5. Which Assistant do you use?

- Amazon Alexa
- Google Assistant
- Apple Homepod
- Other

6. Is your device linked with your account?

- Yes
- Maybe
- No

7. What is the main purpose of your smart speaker?

- Speaker for Music / video audio
- Voice assistant
- Smart Home Controller
- Other

8. How do you enable new skills/abilities?

- By Voice
- By Mobile Device

9. Do you have an experience that different skill/ability encountered rather than the skill you originally wanted?

- I have an experience that I tried to use one skill/ability, but the device presented the other one
• Never experienced

10. Did you try to turn off your device over concerns of security?
   • Yes
   • No

11. Do you have concerns while using your smart speaker?
   • Yes
   • No

12. What is your major concern with smart speaker?
   • Someone can eavesdrop my conversation
   • Leak of my personal information
   • Other

13. Have you used your device to purchase something?
   • Yes
   • No

14. Have you tried to disable the skill/ability that you used before after using it?
   • Yes
   • No

15. What was the reason to disable the skill/ability?

16. Have you accessed device logs or other maintenance/debugging information of your device?
   • Yes
   • No
17. What is the reason that you never accessed those features?
   - Feels Unnecessary
   - Didn’t know how to access
   - Other

18. Do you think an appropriate privacy policy is necessary for skills that collect user’s data?
   (Scaled question between Strongly Disagree to Strongly Agree)

19. Do you read the privacy policies before or during downloading the skills?
   (Scaled question between Strongly Disagree to Strongly Agree)

20. Even though you don’t read the whole privacy policy, would the existence of a privacy policy affect whether you download the application or not?
   (Scaled question between Strongly Disagree to Strongly Agree)

21. Have you experienced trouble with stolen personal information?
   - Yes
   - No

22. What personal information’s security concerns you the most?
   - Address
   - Birth date
   - Security Numbers(SSN, Account Info, etc)
   - Phone number
   - Other

23. Have you ever provided your personal information to your device by speaking to it?
   - Yes
24. Do you use more than one smart device?

- Yes
- No

25. Are you satisfied using the smart devices overall?

(Scaled question between Dissatisfied to Satisfied)

A.2 Awareness

1. Do you use smart speakers, e.g., Amazon Alexa or Google Home?

- Yes
- No

2. How long have you been using the device?

- Less than 1 months
- 1 - 6 months 6 - 12 months
- 1 - 2 years
- More than 2 years

3. What is your gender?

- Male
- Female
- Non-binary / third gender
- Prefer not to say

4. What age group are you?

- Under 18
5. Which Assistant do you use?

- Amazon Aelxa
- Google Assistant
- Apple Homepod
- Other

6. Is your device linked with your account?

- Yes
- Maybe
- No

7. What is the main purpose of your smart speaker?

- Speaker for Music / video audio
- Voice assistant
- Smart Home Controller
- Other

8. Have you used more than one smart speaker?

- Yes
- No

9. Did you feel difference between using those smart speaker market?
• Yes
• No

10. What do you think the most biggest difference?

11. Did you know each platform (market) has different policy requirements?
   • Yes
   • No

12. Do you know your data could be shared with the other third-parties like advertisers?
   • Yes
   • Maybe
   • No

13. Do you know what data type that your device collects for using skills?
   • Yes
   • No

14. Do you know the concept of the smart speakers ‘always listening’?
   • Yes
   • No

15. How do you feel about ‘always listening’?
   (Scaled question between Extremely Uncomfortable to Extremely Comfortable)

16. How are you comfortable with third-parties collecting your data?
   (Scaled question between Extremely Uncomfortable to Extremely Comfortable)

17. How long do you expect the third-party would store your data?
   • Less than 6 months
• 6 - 12 months
• 1 - 2 year
• More than 2 years

A.3 Multi-User

1. Do you use smart speakers, e.g., Amazon Alexa or Google Home?
   • Yes
   • No

2. How long have you been using the device?
   • Less than 1 months
   • 1 - 6 months 6 - 12 months
   • 1 - 2 years
   • More than 2 years

3. What is your gender?
   • Male
   • Female
   • Non-binary / third gender
   • Prefer not to say

4. What age group are you?
   • Under 18
   • 18 - 25
   • 26 - 45
   • 46 - 65
5. Which Assistant do you use?
   - Amazon Alexa
   - Google Assistant
   - Apple HomePod
   - Other

6. Is your device linked with your account?
   - Yes
   - Maybe
   - No

7. What is the main purpose of your smart speaker?
   - Speaker for Music / video audio
   - Voice assistant
   - Smart Home Controller
   - Other

8. How many people in your house use the device?
   - 1
   - More than 2

9. Except you, who else uses smart speaker?
   - Parents
   - Spouse
   - Kids
10. Do you use your smart speaker as a controller of smart home?
   • Yes
   • No

* GUEST *

11. When there are others – that are not your family – around you, does your usage change with the smart speaker?
   • Yes
   • Maybe
   • No

12. Does your guest use your smart speaker? Or was there anyone who tried to use it?
   • Yes
   • Maybe
   • No

13. Do you make your smart speaker turn offed when someone comes to your home?
   • Yes
   • Maybe
   • No

14. Do you change settings of your speaker to protect your privacy when someone is expected to come your home?
• Yes
• No

15. Are you aware that strangers can access to your personal information with your smart device?
   (Scaled question between Strongly Disagree to Strongly Agree)

16. Did one of your guests tried to tell their personal information to your device?
   • Yes
   • No

17. Did it effected your later use of same skill/ability?
   • Yes
   • No

18. Did you deleted the skill/ability because of it after when they are gone?
   • Yes
   • No

19. How comfortable are you if your guests use smart devices without asking?
   (Scaled question between Strongly Uncomfortable to Strongly Comfortable)

* PARENT - KID

20. Do you have kids under the age 13 who uses the device?
   • Yes
   • No

21. Do you test kid’s skills before enabling it for them?
   • Yes
22. Do you check the privacy policies before using the skills for your children?
   • Yes
   • No

23. Do you let your children to download voice assistant applications without asking?
   • Yes
   • Maybe
   • No

24. How comfortable are you with letting your kids using smart speakers alone?
    (Scaled question between Strongly Uncomfortable to Strongly Comfortable)

25. Do you check the log after your kid using it?
   • Yes
   • No

26. Do you experienced to get a violent/sexual content response from your device? (not good for kids)
    • Yes
    • No

27. How do you limit those problems?
    • By muting the device when kids are with the device
    • By not letting kids using the device
    • By disabling the skills

28. If your children are young, do you limit to use the smart devices in front of them?
29. Is there difference of usage when if you are with your kids, and if you are with adults or alone?

- Yes
- No

30. How many times did your device misunderstood you/your children’s command and replied different command?

- Never did
- 1 - 3 times
- 3 - 5 times
- 5 - 10 times
- More than 10 times

31. Was it usually parent’s command or children’s command?

- Parents
- Children
- Similar rate

32. How comfortable are you with if your kids tell personal information during using smart devices?

(Scaled question between Strongly Uncomfortable to Strongly Comfortable)

* ROOMMATES *

33. Do you put your device in your private room or in a common space?

- Yes
34. Do you enable your roommates to use your device?

- Yes
- No

35. Do you share your personal information with them?

- Yes
- Maybe
- No

36. How comfortable are you when your roommates use your smart devices?
   (Scaled question between Extremely Uncomfortable to Extremely Comfortable)

* SMART HOME *

37. How do you think the difficulty of using smart home with your smart device?

- Extremely easy
- Somewhat easy
- Neither easy nor difficult
- Somewhat difficult
- Extremely difficult

38. How many devices can you control with your smart speaker?

- 1 - 2 devices
- 3 - 4 devices
- More than 4 devices
39. Is everyone in your house accessible to smart home?
   - Yes
   - Maybe
   - No

40. Can you limit your device access for your smart home?
   - Yes
   - Maybe
   - No

41. Do you have concern while using it?
   - Yes
   - No

42. What’s the biggest concern while using it?

43. What kind of policies would you like to have to use your smart home with security?

44. Have you ever had arguing with people in your home about using smart home?
   - Yes
   - No

45. Did you have an experience that your guest using your device as a smart home controller?
   - Yes
   - Maybe
   - No
A.4 Developer

1. Have you developed any Alexa skill or Google Action?
   - Yes
   - No

2. Which platform did you developed your skill / action?
   - Amazon
   - Google

3. Can you list two default intents when you create a new skill or action?

4. Can you provide the first line of code in your skill or action code?

5. How does your device’s markets check and test your skills?
   - Before published
   - After published
   - Might or might not

6. Are you aware of required rules of policies of VPA platform? (Such as collecting any personal information from end-users is not allowed, you must provide legally adequate privacy policy within the app and detail page if your application collects personal data.)
   - Yes
   - No

7. How do you get noticed or get checked with those required rules?
   - By searching
   - By notification of platform
8. Why didn’t you searched for the requirements before publishing?
   • Because it doesn’t effect to publish the skill/ability on the platform
   • Doesn’t feel important

9. Do you think an appropriate privacy policy is necessary for skills that collect user’s data?
   • Yes
   • No

10. How important do you think it takes?
    (Scaled question between Extremely Unimportant to Extremely Important)

11. Do you provide valid privacy policy for your skill?
    • Yes
    • No

12. What is the reason that you don’t provide a valid privacy policy?
    • Didn’t know I have to provide the privacy policy
    • Don’t know how to generate a privacy policy

13. Have you copied privacy policies from the other skills? (Including your own skills)
    • Yes
    • Maybe
    • No

14. How do you generate valid privacy policies for your skills?

15. What do you think the most important role of privacy policy?
• Confidence for the skill
• Commitment for end users
• other

16. Have you thought about a program that generates privacy policies?
   • Extremely important
   • Very Important
   • Moderately important
   • Slightly important
   • Not at all important

17. Do you know you cannot ask customers for positive rating?
   • Yes
   • No

18. Have you added a feature to ask your customers for positive rating?
   • Yes
   • No

19. Why did you asked for it?

20. Are you aware of Kids/Health category’s policies of your market?
   • Yes
   • No

21. Are you aware that for Kids/Health category cannot contain toxic/inappropriate content?
   • Yes
22. Have you promoted any products, content, services that directs end users to engage with content outside of Alexa in Kids category skill?
   • Yes
   • No

23. Did you know that violates policy of Alexa?
   • Yes
   • No

24. Are you aware that a Health application must provide a disclaimer in the skill description?
   • Yes
   • No

25. Are you aware you must provide and display a legally adequate privacy policy about the application collects what kind of personal data from end users within the app and on the detail page?
   • Yes
   • No

26. Do you always provide adequate privacy policy for each or your application?
   • Yes
   • No

27. How do you check your application/skill is appropriate with each category’s required policies?
A.5 Fairness

1. While using a smart speaker, have you ever noticed that the device understands other people’s commands better than your own?
   • Yes
   • No

2. Have you ever had a smart assistant better understand anyone of a different gender than you?
   • Yes
   • No

3. Have you ever had a smart assistant better understand anyone of a different race than you?
   • Yes
   • No

4. Have you ever had a smart assistant better understand anyone of a different dialect than yours?
   • Yes
   • No

5. Have you ever had a smart assistant better understand anyone of a different age than you?
   • Yes
   • No

6. Do you think your smart device have a bias with understanding commands within your households?
7. How many times does it misunderstand your/household's command?
   • 1 - 5 times
   • 6 - 10 times
   • More than 10 times

8. Did you experienced problems with misunderstanding command?
   • Yes
   • No

9. What was the problem?

10. Does everyone in your household have the same level of access?
    • Yes
    • No

11. Do you have to change the way you talk to be understood by your smart speaker?
    (For example, pronunciation or speed of speaking)
    • Yes
    • No

12. Have you or anyone you know ever been personally affected due to a misunderstanding by your smart speaker?
    • Yes
    • No

13. What have been the consequences of misunderstandings made by your smart speaker?
Bibliography


