Assessing User Perceptions on the Privacy Implications and Regulatory Efficacy for AI Voice Assistants

Wallace S. Msagusa
College of Engineering
Carnegie Mellon University Africa
Kigali, Rwanda
wmsagusa@andrew.cmu.edu

Isabel Agadagba
School of Computer Science
Carnegie Mellon University
Pittsburgh, Pennsylvania
iagadagb@andrew.cmu.edu

Fernando Ruiloba Portila
College of Engineering
Carnegie Mellon University
Pittsburgh, Pennsylvania
fruiloba@andrew.cmu.edu

Esther Dzifa Mensah
College of Engineering
Carnegie Mellon University Africa
Kigali, Rwanda
emensah@andrew.cmu.edu

ABSTRACT

This research project dives into the privacy opinions and habits of AI voice assistant users. With exponential integration of AI tools in modern software and its lack of regulation, much of the privacy mitigation is left up to the users and their understanding of these technologies' privacy policies. While much has been studied regarding the potential and actual privacy harms caused by voice assistants and the inadequacy of current laws to address these challenges, little has been studied about user perspectives on the role, efficacy and trust in regulation. Studies in this particular area have shown a general distrust among users regarding the security of their personal information, expressing concerns about passive listening and unauthorized data access, and how the perceived corporate social responsibility (CSR), transparency and user backgrounds affect privacy perspectives. As such, we analyze user perceptions towards voice assistants, and possible approaches that maximize privacy and increase trust in these technologies through adequate regulatory measures.

In this experiment, we conduct a user study in the form of an asynchronous survey where we assess users on their usage, opinions and understanding of AI voice assistants, their understanding of privacy risks, how they perceive the potential for privacy harms, and their perception on regulation of such tools.

Keywords

Security, Privacy, Regulation, AI Voice Assistants

1. INTRODUCTION

Voice-based digital assistants (also AI Voice Assistants) have become integral to modern digital ecosystems and they enable individuals to perform a variety of tasks with ease. The widespread adoption of such tools is driven by their ability to offer convenience and personalized user experiences. However, their rapid integration into daily life continues to raise significant concerns regarding information privacy and security [14]. The core functionality of AI Voice Assistants relies on continuous access to vast amounts of personal data, including media files, contact lists, location data and web activity. This data collection and subsequent processing (both locally and remotely) is essential for improving user interactions and enhancing the accuracy of responses, making the voice assistants more useful.

Nevertheless, the pervasive presence of these assistants and their ubiquity in various consumer devices, as noted from different industrial and scholarly works, amplifies the potential risks of data leaks, security breaches, and misuse of personal information. Scholars, regulators and practitioners seem to converge on the idea that user perceptions of privacy and security regarding such tools are critical factors influencing their implementation, adoption, acceptance, compliance and regulation [5, 14]. The Unified Theory of Acceptance and Use of Technology (UTAUT2) model, extended to include privacy concerns and trust, highlights that users' acceptance of AI voice assistants is significantly affected by their perceptions of privacy risks [14].

In this context, our team devised this study built upon findings from different scholarly and industrial works. First, the observation that diverse cultural contexts might play a crucial role in shaping user perceptions with regard to AI voice assistants [14] suggests the need for a more comprehensive understanding of user behavior across different regions and backgrounds.

Secondly, the rising concern about the ethical implications of AI voice assistants, particularly regarding their impact on personal privacy. Documented instances of inadvertent recordings and potential surveillance [13] and worries about unbounded secondary uses and sharing of user data, including by law enforcement agencies demanding access to voice recordings for criminal investigations without probable cause [3] have

highlighted the ethical risks associated with the misuse of these technologies .

Finally, the way that information privacy and security issues surrounding the use of AI voice assistants are further exacerbated by the lack of robust regulatory frameworks to address the challenges they pose. On a general note, regulatory efforts in Europe have been observed to be more proactive. Laws like the European Artificial Intelligence (AI) Act, which came into force on August 1, 2024, exposes companies to "significant penalties for developing, selling, and using risky AI systems" across the 27 European Union member states [1, 8]. The contrast with the slower response seen in the United States and the majority of the world highlights the need for more effective policies, user education and a balance between the convenience of AI voice assistants and the development of privacy-focused designs with “transparent data practices” (as activists in the EU have began calling to prioritize the protection of fundamental human rights when enacting regulatory measures) [9].

With these findings in mind, the team formulated five research questions to gain further insights.

RQ1 : To what extent are end-users aware of privacy implications posed by voice assistant technologies?

RQ2 : What are some of the privacy concerns that end-users have regarding voice assistant usage?

RQ3 : What measures are users of voice assistant technologies putting in place to protect their privacy?

RQ4 : What role do policies and regulation play in enhancing privacy and security of user data with regard to voice assistants?

RQ5 : What are end-users' perceptions on the comprehensibility and efficiency of existing policies and regulatory measures for voice assistants?

To address these questions, we conducted a user study to collect data on user context, awareness, understanding, behavior, and perceptions related to AI voice assistant usage, particularly concerning personal privacy and data security.

This paper also goes further to identify relevant metrics and suggest possible approaches that can be employed to maximize privacy, address civil and human rights concerns, and increase trust in AI voice assistants. For manufacturers, this would inform the design of more transparent data practices and privacy protection approaches, and for policymakers, the insights could potentially provide grounds for appropriate regulatory measures that protect user data and ensure that privacy concerns are adequately addressed.

2. LITERATURE REVIEW

The purpose of the literature review is to highlight the previous findings of how users view and interact with AI Voice assistants in various contexts. We discuss objective and subjective privacy harms that are exacerbated or created through the use of AI voice assistants, as well government and company regulations that have been discussed to mitigate such harms. This background aids us in forming and developing our research questions to expand upon prior findings. We also examine security vulnerabilities that have users concerned and the faulty policy that allows voice assistants wiggle room to invade peoples’ privacy. This helped us as researchers to connect users’ privacy harms with past security breaches and the need for changes in policy to avoid such violations. The selection of academic literature we chose to analyze ranges from user studies, to relevant court case filings, and finally the data collecting methods used by companies advertising AI voice assistant technology.

2.1 Defining AI Voice Assistants

AI voice assistants are sophisticated software programs that utilize artificial intelligence to interpret human speech and respond via synthesized voices [17]. These applications process language to perform tasks such as translation, search the web, hands-free calling and texting, playing music, setting alarms, and more [18, 19]. These technologies can include smart speakers, AI assistants on smartphones, and voice-activated smart TVs [17, 18]. The most popular technologies include Alexa by Amazon, Apple's Siri, Google Assistant, Microsoft's Cortana and Samsung's Bixby [20]. In our study, we decided to measure which of these technologies are being used, and how.

2.2 Widespread Use and Concerns on Voice-Based Digital Assistants

Voice-Based Digital Assistants (VBDA) or AI Voice Assistants are software applications designed to assist users by listening, processing, learning, understanding and responding to voice prompts. These technologies make use of natural language processing and machine learning techniques to perform a range of tasks such as interpreting spoken language, providing weather updates, searching the web, enabling hands-free communication by making calls and sending messages, playing music and setting alarms [4]. The increasing use of these tools in recent years has sparked growing concerns among scholars, authorities, and privacy advocates about their impact on information privacy [6]. Since they require access to personal information for effective functioning, they have massive amounts of personal data such as media, contact lists and browsing history [14]. Other reasons for worry are the ubiquity of such tools in different consumer devices such as speakers, vehicles, TVs, and wearables [14], the increased potential for data leaks, security breaches and data misuse [2, 7, 11], and the lack of effective policies to adequately address the privacy concerns that have arisen [10].

2.3 Privacy Harms and User Perceptions

While these technologies offer convenience and personalized experiences, they also raise significant privacy concerns among users due to their data collection practices, which include sensitive information such as location history and voice queries [14]. Existing literature highlights a general distrust among users regarding the security of their personal information, with many expressing concerns about passive listening and data misuse. The evidence on privacy perceptions is mixed, with various factors influencing how users perceive the risks associated with VBDAs.

In this context, the study by Vimalkumar et al., 2021, highlights the significant privacy issues due to data collection practices and extends the UTAUT2 model by incorporating privacy concerns

and trust as critical factors influencing the adoption of VBDAs [14]. The findings, reached by conducting a quantitative survey across a set of 39 indicators suggest that users' acceptance is significantly affected by their perceptions of privacy risks and the level of trust they have in these technologies. The study also recommends exploring these dynamics in diverse cultural contexts to gain a more comprehensive understanding of user behavior regarding privacy in voice AI technologies. Another article discusses the constant listening for wake words by devices like Alexa, which can inadvertently record private conversations, raising concerns about data misuse, potential surveillance, and ethical implications [11]. It notes the growing awareness of these issues and the regulatory efforts in Europe compared to the slower response in the U.S. The article highlights unresolved issues such as the extent to which users are fully informed of these risks, the effectiveness of opt-out privacy controls, and whether future advancements will improve privacy without sacrificing convenience. It calls for more robust regulatory frameworks, user education, and innovations in privacy-focused voice assistant designs.

2.4 Factors Influencing Privacy Perceptions

Practitioners and scholars seem to agree that there's a number of factors affecting user's perceptions on voice-based digital assistants. It has been observed that privacy perceptions may vary based on technology adoption, smartphone operating systems, and user demographics [5]. This particular study goes further to suggest that users' experiences and backgrounds significantly influence their trust in such tools. For this reason, we thought that adding demographic data in our survey would enrich our study.

Another study that we reviewed analyzed consumer privacy concerns over intelligent voice assistants, examining factors such as perceived corporate social responsibility (CSR), perceived creepiness, and anthropomorphized roles [12]. Findings revealed that high CSR diminishes privacy concerns, while the "servant" role and high perceived "creepiness" of a voice assistant increase privacy concerns. The key result from this study is that privacy concerns significantly affect consumer resistance to using these products. It suggests that companies should reduce creepiness by explaining why information is collected and maximize perceptions of control and trust through opt-in mechanisms. Engaging in public welfare practices can also improve perceived CSR.

Overall, the understanding of user privacy perceptions can inform the design of more transparent data practices and privacy protection approaches. This would enhance user trust and make people more likely to continue using them as they often rely on the collection and/or retention of usage and content data to develop insights that could be used as a knowledge base. For policymakers, the findings indicate the need for appropriate regulatory measures that protect user data and ensure that privacy concerns are adequately addressed.

2.5 Ethical Implications

As noted in other contexts, privacy concerns have surfaced with the advent of voice assistants, highlighted by revelations such as Amazon admitting that workers frequently listen to conversations to enhance their service. This has led to the examination of user privacy in relation to voice assistants, revealing crucial insights into the inherent vulnerabilities of these technologies. Sharif and Tenbergen (2020), identify several significant privacy concerns, including the potential for unauthorized data access and the risk of spontaneous recordings, which can occur even without explicit user activation [13]. This study recognizes the specific risks associated with intelligent voice assistants (IVAs) and underscores the need for privacy protection measures. Increased security, user education, the development of more effective privacy protocols and user-centric design strategies that prioritize data protection are some of the measures that can be used to mitigate these vulnerabilities.

Another more security-focused study provides a comprehensive research map of voice assistants, addressing numerous personal voice assistant (PVA) related topics such as voice authentication (VA), acoustic Denial of Service (DoS), hidden voice commands and acoustic sensing [7]. It also addresses topics such as recording consent. This is useful as it describes the overall PVA ecosystem, including audio processing, speech recognition, and attacks through noise signals. It also provides an exhaustive taxonomy of all the different topics concerning voice assistants and it even provides specific research questions in each area.

2.6 Policy Inadequacy

In a more impactful case concerning governance of voice-based digital assistants, a murder investigation in Arkansas led the police to request voice recordings by an Amazon Echo device hoping it could provide useful information on the events that occurred on the night of the murder [3]. Though Amazon initially refused to provide the information, they eventually conceded and released the required information to authorities. Experts worry that events like this are only the beginning and that current privacy laws are not well equipped to deal with these types of privacy violations. The study goes over the current state of federal and state laws, and the capabilities of voice assistants to record people's conversations inside their own homes and extensively through consumer devices they carry in their pockets. One particularity of the law is that, once information is shared with third parties, there is no reasonable expectation of privacy, meaning that law enforcement is free to collect that information without a warrant. The question on whether the inspection of aggregated digital information amounts to a search is still disputed. The Electronic Communications Privacy Act (ECPA) is a federal statute on technological privacy that prohibits the interception of any wired, oral or electronic communication. The act differentiates between stored and in transit information, and protects some information by requiring a subpoena before being able to search. One part of ECPA that is controversial is that it allows the government to obtain secrecy orders, which prevent technology companies from telling their users that their information is being shared with the government. We found this concerning and the literature we reviewed did not explicitly talk about user awareness with regards to these laws and their privacy implications, so we included user awareness as one of the research questions in our study.

2.7 Users Perceptions on Different Voice Assistant Regulations

While much has been studied regarding the potential and actual privacy harms caused by voice assistants and the inadequacy of current laws to address these challenges, little has been studied about user perspectives in response to government action. Studies

have shown that increased perceived corporate social responsibility, transparency and user backgrounds affect privacy perspectives towards voice assistants, so we believe it would be reasonable to expect similar reactions in response to different governmental regulations. Currently, the law is a gray area, and government actions are not foreseeable ex-ante. This could lead to overconfidence or low trust in users who can't anticipate the role of government when they interact with voice assistants. We plan to analyze user perceptions towards government involvement in the regulation of voice assistants, including existing or hypothetical policies. The hope is that regulators can consider these insights and come up with possible regulatory approaches that better adapt to user needs and perceptions and ultimately maximize privacy and trust in these technologies.

3. METHODOLOGY

We conducted an asynchronous structured survey with 45 participants above the age of 18. The median completion time was 10 minutes and 23 seconds. By making the survey asynchronous instead of live interviews, we aim to obtain data without interference, as well as at the time of the participants discretion. Participants were mainly recruited from Prolific, an online research platform that collects diverse participants whose audience consists of relatively privacy aware individuals. This approach will help ensure respondents are a mix of users with varying levels of privacy knowledge. To incentivize participation, each respondent on Prolific received a $5 reward upon completion of the survey. Participants were also a balance of AI voice assistants users and nonusers, in order to gain understanding of the privacy concerns of those comfortable with such devices, and those who may not be.

Ethical considerations: This project is not approved by the Institutional Review Board (IRB), as this project is strictly for academic purposes. The data collected on each individual, as well as their participation will not be published or previewed outside of the academic context it was designed for, specifically the Privacy, Policy, Law, and Technology fall 2024 course at Carnegie Mellon. We refrain from collecting highly sensitive and identifiable information, such as name, exact age, or gender. We blurred out each participant's email address during the data cleaning and preparation process and stored all other information in a secure google drive folder only accessible by research team members. The Prolific account is only accessed by research team members as well as our academic teaching assistant assigned to our project and professor.

3.1 Study Design and Deployment

The survey consists of 43 demographic and AI voice assistant related questions, including both free response and multiple choice questions. We begin the survey with a detailed description of AI voice assistants to ensure each participant fully understands exactly what devices we are questioning. We include a user friendly definition and list the most common examples of AI voice assistants, further ensuring participants' understanding. We then prompt a multiple choice question regarding AI voice assistant capabilities. This allows us to analyze what percentage of users and nonusers truly understand what an AI voice assistant is and helps identify themselves as users or not.

The main portion of the survey focused on privacy concerns related to AI voice assistants, including data collection, user behavior, device operations, and government involvement. After confirming that participants were familiar with what constitutes an AI voice assistant, we asked them to identify whether they considered themselves users, and to explain why. This information helped us assess how users balance convenience with other privacy-related or unrelated concerns, such as finances, necessity, or access.

Next, the survey asked participants about their specific use of voice assistants and the types of information they allowed these devices to access. Since users' priorities and needs varied, these questions provided insights into the extent to which AI voice assistants were integrated into their homes, and how much control they felt they had—or believed they should have—over these devices.

The following set of questions explored participants' privacy preferences, habits, and concerns. These questions included hypothetical scenarios about their voice assistants and opinions on the regulation of such systems. The responses helped us understand how privacy-conscious users were when using these devices, as well as which company practices raised the most concerns about data security. The final section of the survey focused on demographic information, including education, age range, and geographic location. This data was crucial for categorizing users and making accurate inferences about the broader population.

3.2 Thematic Data Analysis

To identify overarching themes in participants' perceptions of privacy and regulatory efficacy for AI voice assistants, we conducted a thematic analysis of the survey questions. All researchers independently reviewed the responses according to their specific research question or area to identify recurring patterns and themes. We then met to discuss and refine these themes, resolving any disagreements through discussion.

The resulting themes, which include "Awareness of Privacy Risks," "Trust in Technology Companies," and "Desire for Transparent Regulations," are presented in the Results section along with supporting quotes from participants

4. RESULTS

In this section, we present the results of our user study. In order to contextualize our findings, we begin by summarizing the characteristics of our participants, including their demographics and usage of voice assistant products. We then discuss the results concerning each research question. Critical takeaways regarding each research question are shown in bold.

4.1 Participant Characteristics

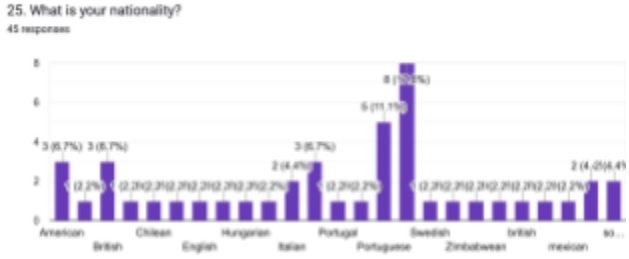

Fig 4.1.1: Participant country of origin

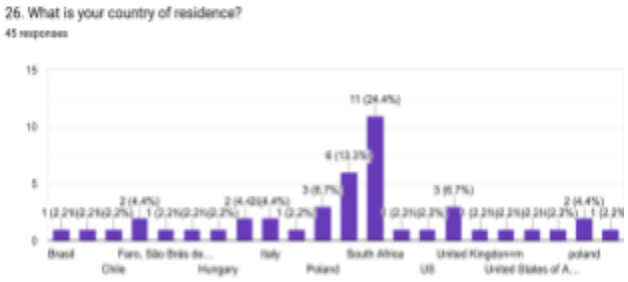

Fig 4.1.2: Participant country of residence

Figures 4.1.1 and 4.1.2 summarize the ethnic demographic characteristics of our participants. Our sample primarily consists of young adults, with the majority (84.4%) being under 40 years old. The largest age group is 30-40 years (31.1%), followed closely by 25-29 years (28.9%) and 18-24 years (24.4%). This demographic distribution aligns with the general trend of AI voice assistant users, who tend to be younger and more tech-savvy. However, the voices of older adults, particularly those over 50, are likely underrepresented in our results, as they account for only 4.4% of the sample.

The most common AI voice assistant used by our participants was Google Assistant (71.1%), followed by Alexa by Amazon (37.8%), Apple's Siri (31.1%), Microsoft's Cortana (11.1%), and Samsung's Bixby (6.7%). The majority (52.9%) of participants have been using voice assistants for 2-4 years, indicating a relatively recent adoption trend. Only 15.6% of participants stated they do not use a voice assistant at all. When asked about their reasons for not using particular voice assistants, most participants cited factors such as uselessness or difficulty of use rather than privacy considerations. For example, one participant stated, "I feel like they are not developed enough in my primary language. It feels awkward and I would rather do it myself as I have more control. It also means there are less errors, and those errors are easily fixed by changing my habits." Another participant responded, "Not comfortable using AI apps; find them useless/confusing."

Interestingly, while only 33.3% of participants reported having formal IT education, a higher percentage (46.7%) indicated having IT work experience. This suggests that many users gain practical knowledge of these technologies through hands-on experience rather than formal training. The majority of participants (71.1%) have been using voice assistants for less than 4 years, with 35.3% adopting the technology within the past year. This recent adoption trend highlights the rapid integration of AI voice assistants into daily life and underscores the need for ongoing research into user perceptions and privacy concerns as these technologies continue to evolve and become more prevalent.

4.2 RQ1: User Awareness

The responses from the survey reveal a mixed level of user awareness about AI voice assistants, with some understanding their mechanisms while others are guided by misconceptions or concerns. For instance, when asked how these systems process commands, many respondents (60%) correctly identified that they interpret and act on spoken language. However, over a fourth of participants (26%) believed the systems rely solely on pre-programmed responses or store all voice data for manual analysis, highlighting gaps in understanding about natural language processing (NLP) and AI voice assistant capabilities. This suggests that while some users are informed about how voice assistants work, others harbor inaccurate or incomplete knowledge, possibly shaped by general apprehension or mistrust.

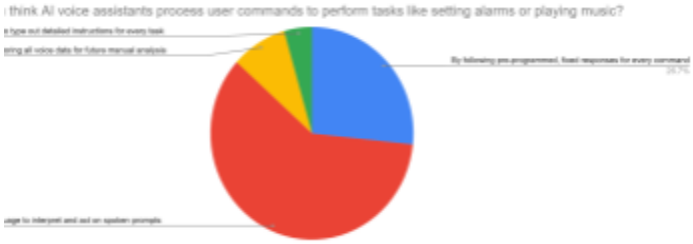

Fig 4.1.1: How users think AI voice assistants work

Patterns in the survey responses indicate a prevalent concern about privacy and data security, which aligns with the high percentage (73.3%) of users believing their devices are always listening. Similarly, nearly half of the participants do not keep their devices active at all times, reflecting cautious behavior. When it comes to sharing personal information, users are more willing to allow access for practical, context-specific purposes like navigation or grocery orders but are hesitant about continuous tracking or sharing sensitive data such as health or banking information. These patterns reflect a cautious approach, with users prioritizing functional utility while maintaining skepticism about long-term data security and privacy practices.

4.2 RQ2: Privacy Concerns

Despite a general lack of awareness, many users express concerns about privacy when using voice assistants. A majority (55.6%) reported apprehensions regarding data collection and usage, with specific worries about data sharing, security, and a lack of transparency .

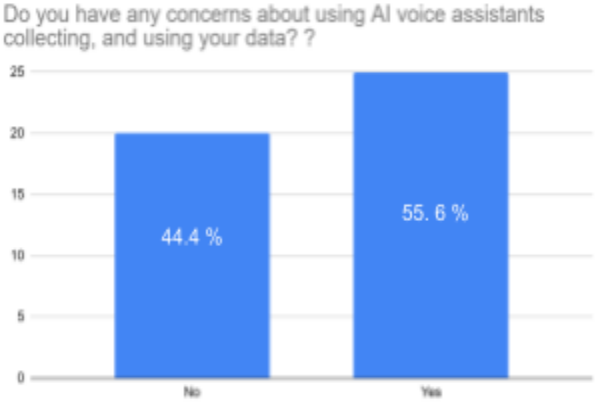

Fig 4.2.1: User concerns about AI voice Assistants

The perception that devices are constantly listening (73.3%) further exacerbates these concerns, indicating a widespread belief in potential surveillance and privacy invasion . However, the data also reveal a paradox: while users express concerns, they often permit access to sensitive information, such as location data and

personal contacts, suggesting a disconnect between awareness and behavior.

Concerns about AI voice assistants and their handling of personal data exhibit a spectrum of severity. At the lower end, users expressed unease about the sheer volume of personal information collected, often citing a lack of transparency about what data is being stored and how it is used. Several respondents mentioned discomfort with the possibility of their data being stored long-term without clarity on its usage, leading to apprehensions about profiling for targeted advertisements. Others highlighted uncertainties about the systems' safety and the trustworthiness of companies managing this data, emphasizing a general mistrust stemming from past breaches or misinformation.

More severe concerns centered on the potential misuse and unauthorized dissemination of sensitive information. Respondents feared their data could fall into the wrong hands, whether through hacking, data leaks, or unauthorized third-party sharing. Some worried about the sale of private information, including health data and personal conversations, to external parties without consent. Additionally, the idea of continuous, unintended recording heightened anxieties, with concerns about sensitive conversations being captured unknowingly. The overarching fear lies in the vulnerability of these systems to breaches and misuse, reflecting an escalating demand for stricter privacy protections and greater accountability from companies handling such data.

4.3 RQ3: User Behaviour

User behavior reflects a complex and sometimes contradictory relationship with privacy and technology. Many users (48.9%) keep their voice assistants active at all times, indicating a level of comfort with continuous listening. Furthermore, while 55% of respondents allow voice assistants access to their location for navigation and weather updates, only 7% permit them to assist with financial transactions. This suggests that users are selectively aware of privacy implications, being more cautious with financial data while being less concerned about other sensitive information. Additionally, only 40% of users actively address their privacy concerns through device settings, indicating a lack of proactive engagement with available privacy controls.

Users reported using voice assistants mainly for setting reminders and alarms (71.1%), playing music (80%), and for educational support and questions (60%). This provides us with a better understanding about user intents and motivations when using this technology. See **Figure 4.3.1**

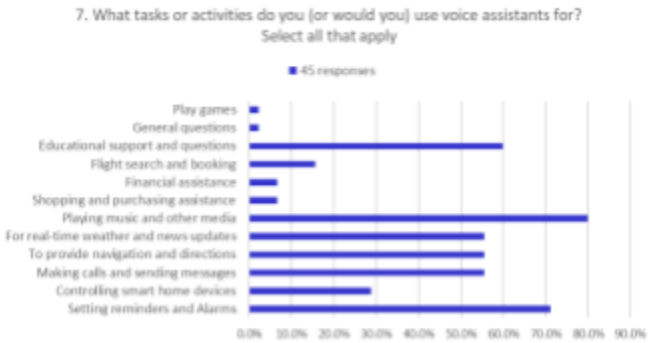

Figure 4.3.1 : What participants use voice assistants for.

The features that users reported to be using the most for protecting their privacy include microphone activation control (55%), data sharing preferences (47.5%), and voice history review and deletion (30%). See Figure

4.4 RQ4 and RQ5: Regulatory awareness

The survey results reveal a significant gap in regulatory awareness among users. A staggering 77.8% of respondents were unaware of any policies governing voice assistant usage in their countries. This lack of awareness correlates with negative perceptions of existing regulations, as 48.9% of participants believe current regulations are ineffective in protecting their privacy. Despite this skepticism, a majority (62.2%) expressed support for stricter regulations, indicating a desire for improved privacy protections. However, trust in government to implement effective regulations is low, with 53.4% of respondents rating their trust at the lowest levels. This highlights a critical need for not only better regulatory frameworks but also for increased transparency and communication from governing bodies regarding privacy protections.

We asked a number of questions to assess the respondents' awareness regarding regulatory frameworks governing voice assistants. The vast majority (77.8%) of respondents were not aware of any policies regulating voice assistant use in their countries. Only 8.9% were aware and 13.3% were unsure. Only 3 respondents (6.6%) were able to provide an actual example of a policy governing privacy, but not specifically voice assistants.

When asked about the efficacy of current regulations for protecting their privacy only 1 person (2.2%) thought that current regulations are effective. 18 persons (40%) were mostly indifferent and 22 persons (48.9%) thought that current regulations were not effective at protecting their privacy.

Despite low user awareness and negative perceptions around current policies, most users (62.2%) thought that regulations could improve their privacy (see **Figure 4.4.1**).

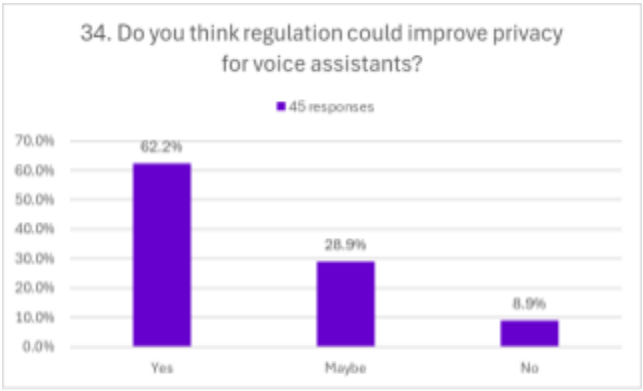

Figure 4.4.1: Participants view on voice assistants

In addition, 34 respondents (75.6%) supported stricter regulations to protect user privacy while using voice assistants. Only 2 respondents (4.4%) did not support stricter regulations and 9 (20%) were unsure. When asked if stricter regulations would increase their confidence when using voice assistants, most participants (62.2%) said yes.

When asked a more open question on how regulations would impact their use of AI voice assistants, most participants also reported that they would be more comfortable while using them. For example, one participant stated "I would trust AI assistants more, which would make me use them more often" in the presence of stricture regulations. 9 respondents (20%) also reported that they would increase their usage of voice assistants. See **Figure 4.4.2**

Figure 4.4.2: Participant,s view on regulatory measures

Participants were asked about what specific features should be regulated and what measures should be taken to address privacy issues. The most popular features that 75.6% of respondents considered should be regulated were: voice recording without consent, personal information collection, and voice usage for unspecified purposes. The most popular measures regulators could take to protect privacy were to require strong security measures (82.2%), to allow users to edit, view and delete collected data from voice assistants (73.3%), and to require companies to disclose what data is collected and shared (71.1%).

Finally, participants were asked how much they trusted the government to provide reasonable regulations to improve privacy for voice assistants. Most respondents (53.4%) answered with the lowest or second lowest score for this measure, meaning that there is little trust in the government.

5. DISCUSSION

The results from the survey gave us important insights into the mind of the median voice assistant user. The responses allowed us to piece together a set of multi-faceted answers to our research questions.

Our findings indicate that end-users have varying levels of awareness regarding the privacy implications of voice assistant technologies (RQ1). Many participants expressed concerns about passive listening and unauthorized data access, echoing the general distrust noted in previous studies. This might be concerning because a lack of information about privacy rights could prevent users from demanding the privacy practices that they are entitled to.

Regarding specific privacy concerns (RQ2), participants frequently mentioned worries about inadvertent recordings of private conversations and potential surveillance. This mirrors the concerns raised by Sharif and Tenbergen (2020), who identified unauthorized data access and spontaneous recordings as crucial privacy risks associated with intelligent voice assistants (IVAs).

The results of this study underscore a critical gap in user understanding of privacy implications associated with voice assistant technologies and their behaviours handling the technology (RQ3). The findings suggest that while users express concerns about privacy, their behaviors often contradict these concerns, revealing a complex relationship between awareness, perception, and action. This disconnect may stem from a lack of education and understanding of the technologies at play, particularly among users with little to no IT knowledge.

Moreover, the low levels of regulatory awareness and trust in existing frameworks indicate a pressing need for more robust policies and clearer communication from regulatory bodies (RQ4). Users are calling for stricter regulations, yet their lack of awareness about current policies suggests that the few existing regulations may not be effectively communicated or enforced. Understandably, users don't believe regulation is effective at protecting their privacy (RQ5). Future studies could focus on the link between privacy policy awareness and trust in privacy policy effectiveness. A big majority of users thought that regulation could have a positive impact on their privacy. This might contrast with other policy areas like content moderation in social media where support for more stringent regulations is divisive[16].

The results highlight the necessity for comprehensive educational initiatives aimed at increasing user awareness of voice assistant technologies and their privacy implications. This could include improving opt-in mechanisms and providing clearer explanations of data collection purposes, as suggested by Mou and Meng (2024). Additionally, there is a clear demand for improved regulatory measures that not only protect user privacy but also foster trust and transparency in the use of AI voice assistants. Addressing these issues is essential for enhancing user confidence and ensuring the responsible use of emerging technologies.

6. LIMITATIONS

The study on AI voice assistants and privacy concerns presents several significant limitations that should be considered when interpreting its results and planning future research in this area.

Self-reported data constitutes a primary limitation of this study. The research relied on participants' own accounts of their perceptions, behaviors, and experiences with AI voice assistants. While this approach provides valuable insights into user perspectives, it is inherently subject to potential biases. Participants may unconsciously alter their responses due to social desirability bias, attempting to present themselves in a more favorable light regarding their privacy practices. Additionally, the accuracy of self-reported data may be compromised by participants' imperfect recall of their actual behaviors or incomplete understanding of the technical aspects of voice assistants. This limitation could potentially lead to a discrepancy between reported privacy concerns and actual privacy-protecting behaviors.

A critical limitation of the study is its relatively small participant pool, consisting of only 45 individuals. This limited sample size restricts the generalizability of the findings to the broader population of AI voice assistant users. The small participant group may not adequately represent the diverse range of user demographics, cultural backgrounds, technological literacy levels, and usage patterns that exist among the global user base of voice assistants. This limitation is particularly significant given the study's acknowledgment of the potential influence of diverse cultural contexts on shaping user perceptions of AI voice

assistants. The restricted sample size may have prevented the researchers from identifying important variations in privacy concerns or behaviors across different user segments.

Another notable limitation is the lack of an in-depth analysis of the privacy policies specific to AI voice assistants. This omission represents a missed opportunity to provide a comprehensive understanding of the legal and ethical frameworks governing these technologies. Without a thorough examination of these policies, the study may not fully capture the alignment (or misalignment) between user perceptions and the actual privacy protections offered by voice assistant providers. This gap in the research limits its ability to offer concrete recommendations for policy improvements or to assess the adequacy of current privacy safeguards.

7. CONCLUSION

We conducted a survey with 45 participants to investigate five research questions: 1)To what extent are end-users aware of privacy implications posed by voice assistant technologies? 2)What are some of the privacy concerns that end-users have regarding voice assistant usage? 3)What measures are users of voice assistant technologies putting in place to protect their privacy? 4)What role do policies and regulations play in enhancing privacy and security of user data with regard to voice assistants? 5)What are end-users' perceptions on the comprehensibility and efficiency of existing policies and regulatory measures for voice assistants? Participants responded with a medley of opinions, behaviours, and thoughts concerning their experience with AI voice assistants. A majority of participants expressed concerns about data privacy, including unauthorized data sharing and selling, and stated restricting access to sensitive information such as health and banking information However, most participants behaved in a contradictory and trusting manner with their device like allowing it to access location data and eating habits. Less than half of our participants admitted to addressing their concerns with their privacy settings while the vast majority rated their experience using these privacy settings from very easy to average difficulty. Respondents agreed on the increase of privacy regulations for companies aggregating and storing voice data, mentioning the lack of strict standards in this industry. We examined these answers and addressed possible solutions to participants' concerns with further areas of research in our closing discussion.

8. REFERENCES

[1] AI Act enters into force - European Commission: *https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en*. Accessed: 2024-11-11.[1]

[2] Alepis, E. and Patsakis, C. 2017. Monkey Says, Monkey Does: Security and Privacy on Voice Assistants. *IEEE Access*. 5, (2017), 17841–17851. DOI:https://doi.org/10.1109/ACCESS.2017.2747626.

[3] ALEXA, WHAT SHOULD WE DO ABOUT PRIVACY? PROTECTING PRIVACY FOR USERS OF VOICE ACTIVATED DEVICES - Document - Gale Academic OneFile: *https://go.gale.com/ps/i.do?p=AONE&u=cmu_main&id=GALE%7CA537852821&v=2.1&it=r&aty=ip*. Accessed: 2024-11-01.

[4] Aw, E.C.-X. et al. 2022. Alexa, what's on my shopping list? Transforming customer experience with digital voice assistants. *Technological Forecasting and Social Change*. 180, (Jul. 2022), 121711. DOI:https://doi.org/10.1016/j.techfore.2022.121711.

[5] Awojobi, B. and Landry, B. 2023. An Examination of Factors Determining User Privacy Perceptions of Voice-Based Assistants. *International Journal of Management, Knowledge and Learning*. 12, (Feb. 2023). DOI:https://doi.org/10.53615/2232-5697.12.53-62.

[6] Bolton, T. et al. 2021. On the Security and Privacy Challenges of Virtual Assistants. *Sensors*. 21, 7 (Mar. 2021), 2312. DOI:https://doi.org/10.3390/s21072312.

[7] Cheng, P. and Roedig, U. 2022. Personal Voice Assistant Security and Privacy—A Survey. *Proceedings of the IEEE*. 110, 4 (Apr. 2022), 476–507. DOI:https://doi.org/10.1109/JPROC.2022.3153167.

[8] EU takes modest step as AI law comes into effect: 2024. *https://www.amnesty.eu/news/statement-eu-takes-modest-step-as-ai-law-comes-into-effect/*. Accessed: 2024-11-11.

[9] EU's AI Act fails to set gold standard for human rights: *https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/*. Accessed: 2024-11-11.

[10] Liao, S. et al. 2020. Measuring the Effectiveness of Privacy Policies for Voice Assistant Applications. *Annual Computer Security Applications Conference* (Austin USA, Dec. 2020), 856–869.

[11] Lynskey, D. 2019. "Alexa, are you invading my privacy?" – the dark side of our voice assistants. *The Guardian*.

[12] Mou, Y. and Meng, X. 2024. Alexa, it is creeping over me – Exploring the impact of privacy concerns on consumer resistance to intelligent voice assistants. *Asia Pacific Journal of Marketing and Logistics*. 36, 2 (Jan. 2024), 261–292. DOI:https://doi.org/10.1108/APJML-10-2022-0869.

[13] Sharif, K. and Tenbergen, B. 2020. Smart Home Voice Assistants: A Literature Survey of User Privacy and Security Vulnerabilities. *Complex Systems Informatics and Modeling Quarterly*. 24 (Oct. 2020), 15–30. DOI:https://doi.org/10.7250/csimq.2020-24.02.

[14] Vimalkumar, M. et al. 2021. 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*. 120, (Jul. 2021), 106763. DOI:https://doi.org/10.1016/j.chb.2021.106763.

[17] HONOR. 2024. Mastering AI Voice Assistants in 2024: A Complete Guide. HONOR Blog. (Jul. 2024) https://www.honor.com/ph/blog/what-are-ai-voice-assistants-and-how-they-work/.

[18] Aisera. 2024. AI Assistant | Best Types and Key Features for Work Productivity. Aisera. (Nov. 2024)https://aisera.com/chatbots-virtual-assistants-conversational-ai/.

[19] Infobip. 2024. AI Voice Assistants: Everything you need to know. Infobip Blog. (Aug. 2024) https://www.infobip.com/blog/ai-voice-assistants.

[20] TechTarget. 2024. What is a Virtual Assistant (AI Assistant)? TechTarget. (Sep. 2024) https://www.techtarget.com/searchcustomerexperience/definition/virtual-assistant-AI-assistant

9. APPENDIX

A SURVEY INSTRUMENT

Italicized text is used to indicate survey flow and response type. Answer choices are shown in bullets below each question. Answer responses with the text "please specify" or "please describe" included a free response box for participants' to explain their answer.

Q1: How do you think AI voice assistants process user commands to perform tasks like setting alarms or playing music?

- By following pre-programmed, fixed responses for every command
- By processing language to interpret and act on spoken prompts
- By recording and storing all voice data for future manual analysis
- By requiring users to type out detailed instructions for every task

Q2: Do you use AI voice Assistants?

- Yes
- No
- I'm not sure

Q3: If not, why do you not use them? *(Free response field) Question displayed if answer to Q2 is "No".*

Q4: How long have you been using voice assistants? *Question displayed if answer to Q2 is "Yes".*

- <1 year
- 2-4 years
- 5-7 years
- 8-10 years
- 10+ years

Q5: Which Voice assistant do you use and/or prefer? Select all that apply.

- Alexa by Amazon
- Apple's Siri
- Google voice Assistant
- Microsoft's Cortana
- Samsung's Bixby
- other : _____

Q6: Why do you prefer using these voice assistants? *(Free response field)*

Q7: What tasks or activities do you use voice assistants for? Select all that apply?

- Setting reminders and Alarms
- Controlling smart home devices (thermostat, door lock, lights, etc.)
- Making calls and sending messages
- To provide navigation and directions
- For real-time weather and news updates
- Playing music and other media
- Shopping and purchasing assistance
- Financial assistance[to track spending, manage budgets , automate and set up payments]
- Flight booking and searching assistance
- Educational support and asking questions
- Other (please specify) *(Free response field)*

Q8: Do you keep your voice assistant active at all times?

- Yes [it is always active]
- No [it is inactive when not in use]
- I'm not sure

Q9: What personal information do you (or would you) allow your voice assistant to have access to? (location data, names, bank accounts for purchasing capabilities, etc.)

- Would you let your voice assistant have information on your eating habits to make food delivery or grocery orders?
- Would you allow your Voice assistant to track your location when using it for navigation purposes? Would you allow it to continuously track you or only when in use?
- Would you allow your voice assistant to have access to your banking information to make approved purchases on your behalf? What about recurring charges?
- Would you allow your voice assistant to have access to your list of contacts so that it can make automatic calls or send messages on your behalf ?
- Would you be willing to share your health history with your voice assistant to notify you of prescription or medical testing updates?

Q10: Do you think your device is listening to you at all times?

- Yes
- No

Q11: Do you have any concerns about using AI voice assistants collecting, and using your data? ?

- Yes
- No

Q12: If yes (above), what concerns do you have about AI voice assistants collecting, and using your data? *(Free response field)*

Q13: If you have any concerns, are you doing anything to address such concerns?

- Yes
- No

Q14: If yes, what are you doing? *(Free response field)*

Q15: Do you know if the voice assistant(s) you're using have any privacy settings?

- Yes
- No

Q16: If yes (above), do you use any privacy settings for your voice assistant?

- No
- Yes. (Please specify)

Q17: On a scale of 1 to 5, how easy was it to access and use the privacy settings? (1 - Very Easy, 2 - Easy, 3 - Average, 4 - Difficult, 5 - Very Difficult)

- 1
- 2
- 3
- 4
- 5

Q18: Did putting such settings in use break any functionality?

- Yes
- No
- I don't know

Q19: If yes, what functionality did it break?*(Free response field)*

Q20: If yes (above), did you have to change how you use the assistant for particular tasks?

- Yes
- No

Q21: If you have privacy concerns, what do you think could be improved for voice assistants to address such concerns?*(Free response field)*

Q22: If you had the opportunity to unlock more functionality, would you allow your voice to be recorded and sent to a server so that the company can use it to improve a service for you?

- Yes
- No
- Maybe/ Not sure

Q23: Would you use your voice for tasks that involve sensitive personal information, like your credit card number or your health?

(Some scenarios could include:

- Allow your voice assistant to make online purchases for you through accessing your personal banking information.
- Allowing the voice assistant to approve recurring purchases.
- Allowing the voice assistant to monitor your health status, manage consultations and access your insurance information.)
  - Yes
  - No
  - Maybe

Q24: On a scale of 1 to 5, 5 being very concerned, how concerned are you about voice identification without explicit consent for the following settings? (Voice identification is a technology that uses a person's diction to identify, authenticate, and distinguish them.)

- 1
- 2
- 3
- 4
- 5

Q25: When not directly interacting with a voice assistant at home

- 1
- 2
- 3
- 4
- 5

Q26: When calling a service provider, such as a bank or utility company

- 1
- 2
- 3
- 4
- 5

Q27: When not directly interacting with a voice assistant application on your phone

- 1
- 2
- 3
- 4
- 5

Q28: When interacting with a government service on the phone

- 1
- 2
- 3
- 4
- 5

Q29: When having a conversation in a public space

- 1
- 2
- 3
- 4
- 5

Q30: Are you aware of any current regulations or laws that govern the use of AI voice assistants?

- Yes (Mention) *(Free response field)*
- No
- Maybe

Q31: Do you think regulation could improve privacy for voice assistants?

- Yes
- No

Q32: Which of the following do you think should be addressed through regulation? (Select all that apply)

- Voice identification
- Voice recording without consent
- Targeted ads from voice recordings
- Personal information collected through voice assistants

Q33: What do you think is the most important issue concerning privacy in voice assistants? *(Free response field)*

Q34: On a scale from 1 to 5 (1 signifying no trust and 5 signifying complete trust), how much do you trust the government to provide sensible regulations to improve privacy for voice assistants

- 1
- 2
- 3
- 4
- 5

Q35: How effective do you believe current regulations are in protecting your privacy when using AI voice assistants on a scale of 1 to 5 (1 having no effect and 5 being fully effective) ?

- 1
- 2
- 3
- 4
- 5

Q36: Do you support the implementation of stricter regulations to protect user privacy and data security for AI voice assistants?

- Yes
- No

Q37: What is your nationality?*(Free response field)*

Q38: What is your country of residence?*(Free response field)*

Q39: What is your current occupation?*(Free response field)*

Q40: What age bracket do you fall in?

- 18 - 24
- 25 - 29
- 30 - 40
- 40 -50
- 51 and above

Q41: What is your highest level of education?

- High school
- Undergrad
- Masters
- Phd

Q42: Do you have a formal education in a computer-related field, such as computer science or IT?

- Yes
- No

Q43: Do you have work experience in a computer-related field , such as computer science or IT?

- Yes
- No