MAKING VOICES HEARD

VOICE INTERFACES AND PRIVACY

Literature Surveys

Making Voices Heard
Literature Surveys: Voice Interfaces and Privacy

Research and Writing **DIVYA PINHEIRO, SHWETA MOHANDAS**
Review and Editing **SAUMYAA NAIDU, PUTHIYA PURAYIL SNEHA, PRANAV MANJESH BIDARE**
Research Inputs **SUMANDRO CHATTAPADHYAY**
Copyediting **THE CLEAN COPY**
Illustration **KRUTHIKA N.S.**
Report Layout and Design **SAUMYAA NAIDU**

CENTRE FOR INTERNET AND SOCIETY
Supported by Mozilla Corporation

Contents

1. Background

Efforts to develop technologies with voice recognition have been ongoing since the 1960s. Though significant advances in this field were seen in the 1990s with the advent of personal computers (PCs), the biggest breakthrough was the introduction of Siri (a voice-based virtual assistant) on the Apple iPhone in 2011. The use of voice-controlled technologies is not limited to mobile phones and smart speakers; now, they are also integrated with other smart devices such as PCs (as in the case of Microsoft's Cortana), TVs, and cars.[1]

However, the increased use of voice interfaces (VIs) has led to the emergence of a host of concerns, specifically surrounding user privacy. According to a 2020 study, about 33% of adults surveyed reported that privacy concerns were a top reason for not purchasing devices with built-in VI systems; this figure saw a significant increase from 16% in 2018 and 23% in 2019.[2] This article aims to analyse the privacy concerns surrounding VIs, both now and in the future.

2. The spectrum of VI devices

The wide prevalence of microphone-enabled devices today has ushered in an "era of Ubiquitous Listening".[3] VI devices can be categorised into three kinds –

- Manually activated devices – The person presses a button that causes the device to turn on and begin recording.
- Speech-activated devices – These devices remain in an inert state of passive processing. The device re-records local information without transmitting or storing any information and only begins actively recording when it detects its trigger word or 'wake word',[4] such as 'Hey Siri' or 'Ok Google'.
- Always on devices – These devices are designed to record and transmit data all the time until turned off.[5]

Privacy concerns arise, particularly, in the latter two categories, where devices can access, record, and store the data of the individual.[6] Most people do not

1 Youval Nachum, "Privacy Issues with Voice Interfaces", *EEWeb*, 1 July 2019, **https://www.eeweb.com/privacy-issues-with-voice-interfaces/**.

2 Bret Kinsella, "Privacy Concerns Rise Significantly as 1-in-3 Consumers Cite It as a Reason to Avoid Smart Speakers", *Voicebot.ai*, 11 May 2020, **https://voicebot.ai/2020/05/11/privacy-concerns-rise-significantly-as-1-in-3-consumers-cite-it-as-reason-to-avoid-smart-speakers/**.

3 David Talbot, "The Era of Ubiquitous Listening Dawns", *MIT Technology Review*, 8 August 2013. **http://www.technologyreview.com/news/517801/the-era-of-ubiq-uitous-listening-dawns/**.

4 Stacey Grey, *Always on: Privacy Implications of Microphone-Enabled Devices*, Future of Privacy Forum, 16 April 2016, **https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf**.

5 Grey, Always on: Privacy Implications of Microphone-Enabled Devices.

6 Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, David Wagner, "Privacy Attitudes of Smart Speaker Users", *Proceedings on Privacy Enhancing Technologies*, 2019, no. 4 (2019), 250–271.

understand when a VI is listening and where their data is being stored.[7] The data thus collected is often exploited for targeted advertising.[8] Patent filings at the United States Patent and Trademark Office (USPTO) indicate an increase in the development of always-on devices that listen to things beyond the device's wake word to perform increasingly sophisticated analysis.[9]

3. Primary concerns related to privacy

The same features of speech recognition that make such devices appealing are also those that give rise to privacy concerns as VIs become increasingly integrated with our daily lives.[10] Though such services typically require user permission to work, it is usually granted if people are interested in its use.[11] A survey of Android users found that only 17% of respondents paid attention to permissions during app installations and only 3% were able to answer questions on these permissions.[12] Unlike phones or devices that are used by specific individuals, VIs such as Google Home and Amazon Echo can collect data from people who have not consented to their conversation being recorded. This could include visitors, workers, and even children.

3.1. Listening in to private conversations

One of the main issues concerning voice-based virtual assistants is that the device can be activated through the accidental use of wake words. This constant listening has raised concerns regarding devices eavesdropping on private conversations as well as the processing and sharing of data with third parties including law enforcement agencies.[13]

The Supreme Court of India recognised the right to privacy as implicit in the right to life and liberty under Article 21. This includes the right to be left alone. A citizen has the right to safeguard their own privacy as well as that of their family, educational details, etc. Such information can only be published with the person's

7 Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. "'What Can't Data Be Used For?' Privacy Expectations about Smart TVs in the US", *Proceedings of the Third European Workshop on Usable Security*, 23 April 2018, https://www.ndss-symposium.org/wp-content/uploads/2018/06/eurousec2018_16_Malkin_paper.pdf.

8 John M. Simpson, "Home Assistant Adopter Beware: Google, Amazon Digital Assistant Patents Reveal Plans for Mass Snooping", *Consumer Watchdog*, 2017.

9 Nathan Malkin, Serge Egelman, and David Wagner, "Privacy Controls for Always-listening Devices", *Proceedings of the New Security Paradigms Workshop*, 2019, 78–91.

10 Stacey Grey, Always on: Privacy Implications of Microphone-Enabled Devices, Future of Privacy Forum, 16 April 2016, https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

11 Dan Arp, Erwin Quiring, Christian Wressnegger, and K. Rieck, "Privacy Threats through Ultrasonic Side Channels on Mobile Devices", 2017 *IEEE European Symposium on Security and Privacy*, 2017, pp. 35–47.

12 Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner, "Android Permissions: User Attention, Comprehension, and Behavior", in *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS 2012)* (ACM Press, 2012).

13 Sidney Fussell, "Police Want Your Smart Speaker—Here's Why", *Wired*, 23 August 2020, https://www.wired.com/story/star-witness-your-smart-speaker/.

consent.[14] One of the major privacy concerns associated with the use of constantly listening VIs is that there is a high chance of third parties listening in on private conversations through the device.

These devices mostly record information on hearing the wake word. However, people may unintentionally cause the device to begin recording if a word similar to the wake word is spoken. A study found that more than 1,000 terms can activate VI devices, highlighting the scope of the potential risk to privacy.[15] The phrases were not just limited to those that sounded very similar to the wake words, but also remote words such as 'unacceptable' (to which Alexa was activated) and 'tobacco' (to which Echo was activated). This finding is further reiterated by the results of a study that found that VI devices were accidentally activated by 64% of people using it, in a month.[16]

Recently, it was revealed that the big five tech companies – Amazon, Apple, Facebook, Alphabet/ Google, and Microsoft – have been using human contractors to analyse a small percentage of VI recordings. These recordings, although anonymous, can potentially contain personal information, resulting in an infringement of user rights.[17] A report also found that the information passed on included sensitive personal information such as the latitude and longitude coordinates associated with the voice data, which could indicate a person's home address.[18]

Third-party access to the personal information of individuals not only raises questions regarding privacy but also paves the way for other uses of this data such as for profiling and surveillance.

3.2. Access and use of VI data by law enforcement

Digital data has become increasingly useful to law enforcement and security agencies, with the police relying on wearables and smart devices to verify the claims of people made during an investigation.[19] The first instance of the use of VI data as evidence was in a 2015 murder case in the United States, in which a man was found dead in a hot tub. Investigators issued a warrant to Amazon, requiring the company to turn over information and audio recordings captured by the suspect's Echo

14 *R Rajagopal v. State of T.N.* (1994) 6 SCC 632, pp. 649–51.

15 Eric Hal Schwartz, "More than 1,000 Phrases Will Accidentally Awaken Alexa, Siri, and Google Assistant: Study", *Voicebot.ai*, 6 July 2020, **https://voicebot.ai/2020/07/06/more-than-1000-phrases-will-accidentally-awaken-alexa-siri-and-google-assistant-study/**.

16 Eric Hal Schwartz, "Voice Assistants Accidentally Awakened by 64% of Users a Month: Survey", *Voicebot.ai*, 9 January 2020, **https://voicebot.ai/2020/01/09/voice-assistants-accidentally-awakened-by-64-of-users-a-month-survey/**.

17 Dorian Lynskey, "'Alexa, Are You Invading My Privacy?' – The Dark Side of Our Voice Assistants", *The Guardian*, 9 October 2019, **https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants**

18 Sarah Perez, "41% of Voice Assistant Users Have Concerns about Trust and Privacy, Report Finds", *TechCrunch*, 25 April 2019, **https://techcrunch.com/2019/04/24/41-of-voice-assistant-users-have-concerns-about-trust-and-privacy-report-finds/**.

19 Fussell, "Police Want Your Smart Speaker", *Wired*.

speaker.[20] VI devices have since been used both to exonerate[21] as well as to hold suspects guilty of crimes.[22]

This risks creating a culture of state surveillance of the daily activities of citizens with potentially worrying consequences.[23] As more of such data is collected, we must ensure that it receives robust protection.[24]

3.3. Data used for advertisement strategies

VI manufacturers use the data collected from people using the devices to enhance their advertisement strategies. Patents filed in the United States reveal how these devices can be used for massive information collection and intrusive digital advertising.[25] Such data is collected on the pretext of providing customers with advertisements customised to their interests.[26] VIs greatly benefit advertisers who rely on complex data sets to make essential advertising decisions. The massive amount of data gathered from app and platform VI interactions allow for efficient processing, analysis, and access of data.[27] Although the practice is currently uncommon, and manufacturers currently have policies that specifically restrict advertisements on VI devices, there is potential for their use as a mode of advertisement that informs users of content that caters to their interests.[28]

3.4. The privacy of children on VI devices

Two-thirds of India's internet users are in the 12–29 years age group, with those in the 12–19 age group accounting for about 21.5% of the total internet usage in metro cities.[29] Children today utilise the internet to access information, education,

20 "Servant or Spy? Law Enforcement, Privacy Advocates Grapple with Brave New World of AI Assistants", *CNBC*, accessed 24 November 2021, https://www.cnbc.com/2017/01/06/servant-or-spy-law-enforcement-privacy-advocates-grapple-with-brave-new-world-of-ai-assistants.html.

21 Kayla Epstein, "Police Think Amazon's Alexa May Have Information on a Fatal Stabbing Case", *Washington Post*, 3 November 2019, https://www.washingtonpost.com/technology/2019/11/02/police-think-amazons-alexa-may-have-information-fatal-stabbing-case/

22 Juang,"Servant or Spy?",*CNBC*

23 Garfield Benjamin, "Amazon Echo's Privacy Issues Go Way Beyond Voice Recordings", *The Conversation*, 21 January 2020, https://theconversation.com/amazon-echos-privacy-issues-go-way-beyond-voice-recordings-130016.

24 Joseph Jerome, "Alexa, Is Law Enforcement Listening?" *Center for Democracy and Technology*, 4 January 2017, https://cdt.org/insights/alexa-is-law-enforcement-listening/.

25 John M. Simpson, "Home Assistant Adopter Beware: Google, Amazon Digital Assistant Patents Reveal Plans for Mass Snooping", *Consumer Watchdog*, 13 December 2017, https://www.consumerwatchdog.org/privacy-technology/home-assistant-adopter-beware-google-amazon-digital-assistant-patents-reveal.

26 Simpson, " Home Assistant Adopter Beware", *Consumer Watchdog*.

27 Jason Hall, "How Artificial Intelligence is Transforming Digital Marketing", *Forbes*, accessed 24 November 2021, https://www.forbes.com/sites/forbesagencycouncil/2019/08/21/how-artificial-intelligence-is-transforming-digital-marketing/?sh=39700bde21e1.

28 Jesus Martín, "Advertising in Voice Interfaces", *UX Collective*, 14 July 2020, https://uxdesign.cc/advertising-in-voice-interfaces-4b1ca14fa28b

29 Neilsen, "Digital in India 2019 – Round 2 Report", *IAMAI*, accessed 24 November 2021, https://reverieinc.com/wp-content/uploads/2020/09/IAMAI-Digital-in-India-2019-Round-2-Report.pdf.

and other opportunities.[30] The risk to privacy is one of the primary concerns pertaining to children's use of the internet. Children on the internet are less likely to have a comprehensive understanding of the consequences of privacy infringement, making them a vulnerable group that needs added protection.[31]

Chapter IV of the Personal Data Protection Bill, 2019 (PDP), lays down special conditions for the processing of a child's data. Such processing must be done with the intention of ensuring the best interests of the child after taking appropriate steps to verify their age and on receiving the consent of a parent or guardian.[32] The European Union's General Data Protection Regulation (GDPR)[33] and the Children's Online Privacy Protection Rule (COPPA)[34] in the United States also provide similar protections. These provisions have, however, not laid down explicit consequences for non-compliance with these rules; the Federal Trade Commission in the US has been slow to impose hefty fines for such acts and the still-young GDPR has not dealt extensively with such issues.[35]

4. Voice biometrics and the future steps for voice technologies

One of the more recent advancements in this area is the use of voice biometrics to authenticate the person using the device. Voice biometrics require that the system first process a voice sample to extract speaker-specific characteristics to build a statistical model, referred to as a voiceprint or a voice signature. Following this, any new input is compared with the existing voice signature for verification.[36] Data collected through VIs may also fall within the purview of biometric data. The Supreme Court of India, in the landmark case of *Justice Puttaswamy v. Union of India*, characterised biometric data as that which is intrinsically linked to humane characteristics.[37] The Personal Data Protection (PDP) Bill classifies biometric data as sensitive personal data that requires explicit consent for processing.[38]

Voice biometrics seem to be the proposed way forward for VIs. Google has confirmed that it is working on a new Google Assistant feature that can be used

30 UNICEF, "The State of the World's Children 2017. Children in a Digital World", 2017, https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

31 Sonia Livingstone, "Children: A Special Case for Privacy?" *International Institute of Communications*, 19 December 2019, http://www.iicom.org/intermedia/intermedia-july-2018/children-a-special-case-for-privacy.

32 Section 16, Personal Data Protection Bill, 2019.

33 General Data Protection Regulation (GDPR), https://gdpr-info.eu/.

34 Federal Trade Commission, "Children's Online Privacy Protection Rule", https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

35 Martyn Farrows, "Let's Talk Voice Tech, Data Privacy, and Kids", *VoiceBot.AI*, 28 March 2020, https://voicebot.ai/2020/03/28/lets-talk-voice-tech-data-privacy-and-kids/.

36 Abhijit Ahaskar, "Voice Biometrics Are Cleverer Now, But Still Need More Work", *LiveMint*, 6 February 2020, https://www.livemint.com/technology/tech-news/voice-biometrics-are-cleverer-now-but-still-need-more-work-11581011267941.html.

37 *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.

38 Section 3(7), (Draft) Personal Data Protection Bill, 2019.

to authorise financial transactions through voice biometrics.[39] Unlike identifiers such as phone numbers, address or email ids, biometrics cannot be discarded or replaced. This raises significant privacy issues relating to how such data are collected, processed, and stored. The data may be used for purposes other than that for which they were initially collected (a phenomenon also known as function creep).[40]

Recent advancements in technology pose threats to the privacy of individuals who make use of these services. This issue becomes particularly relevant when dealing with an individual's personal information or the information of people whose consent has not been obtained, such as children or people who are excluded from going through the privacy policies due to accessibility reasons or old age.

5. Conclusion

While VIs provide not just convenience but also an easier way to navigate the internet for some people, concerns around privacy and data protection loom large. While there is a need for VIs that are better at understanding the consumer, there is also a need to understand how these systems get their training data. With more voice technologies moving to always listening systems that can send targeted ads and use voice as a verification and identification system, there is a need to look closely at the privacy risks resulting from the collection, usage, and processing of voice data.

39 Ryne Hager, "Google Confirms New Voice Confirmation Feature for Purchases in Assistant", *Android Police*, 25 May 2020, **https://www.androidpolice.com/2020/05/25/google-assistant-gets-new-confirm-with-voice-match-setting-for-payments/**.

40 Digidentity. "Privacy or Security? 'Function Creep' Kills Your Privacy", retrieved October 17, 2020, **https://www.digidentity.eu/en/article/Function-creep-kills-your-privacy/**