Data Protection and Privacy
25th February 2025



Idorenyin Ekpenyong[1]

THE PRIVACY RISKS OF VOICE-ACTIVATED DEVICES: SAFEGUARDING PERSONAL INFORMATION IN THE DIGITAL AGE

1. Introduction

1.1 The evolution of voice-activated devices is a testament to human ingenuity and technological advancement. In its infancy, it was a mere novelty, limited in capability and accuracy. Today, it has blossomed into an intelligent, responsive, and highly intuitive part of our daily lives offering convenience through hands-free control, smart home automation, and personalized assistance. It began with simple voice commands for dialing phones and has now expanded into sophisticated systems that control our homes, assist in our work, and even conversationally interact with us. This leap was made possible by advancements in artificial intelligence and machine learning, enabling devices to understand, learn, and respond to human speech in a remarkably nuanced way.[2]

1.2 However, their growing presence raises significant concerns about data privacy and security. Voice-activated devices can potentially record and store sensitive information, making them vulnerable to hacking and data breaches. Therefore, protecting your privacy and security captured/channeled through voice-assisted devices is essential. These

---

[1] **Idorenyin Ekpenyong, Associate, Intellectual Property and Technology Department, S.P.A. Ajibade & Co., Lagos, Nigeria.**

[2] OrCam Staff, 'Voice-Activated Devices: Making Technology Accessible for Visually Impaired Individuals' available at <https://www.orcam.com/en-us/blog/voice-activated-devices> last accessed 21 February 2025.

devices continuously listen for activation commands, often collecting and storing sensitive personal information, which can be exploited if not adequately protected.

1.3 This article will explore the risks associated with voice-activated devices, including unauthorized data collection, third-party access, and potential cyber threats. It will also examine regulatory frameworks governing voice data privacy. Finally, it will recommend best practices for users to safeguard their personal information, such as managing privacy settings, limiting data sharing, and using secure networks. By understanding the vulnerabilities of voice technology, individuals and organizations can make informed decisions to protect their data while benefiting from the convenience of smart devices.

2. Understanding Voice-Activated Devices.

2.1 Voice activation technology is a software program or hardware device that can decode the human voice, sometimes referred to as voice recognition or speech recognition software. This technology has become more and more popular in recent years among everyday consumers. Although using voice recognition technology is as simple as uttering a few words or issuing some commands, the way it works is quite complex. First, speech recognition software filters through the sounds we speak and translates them into a format it can read. Then, it analyzes that translation for meaning and uses that information, along with its algorithm and previous inputs to guess what we say. Personal voice-activated devices understand us and improve their ability to filter our voices over time, becoming more and more accurate in voice processing with regular use. It gets complex when accounting for other users, different languages and dialects, and the other factors that can affect human speech such as background noise or vocal inflexions. These factors can affect how voice-activated technology understands a speaker.

2.2 Voice-activated technology uses digital Assistants such as *Amazon's Alexa*, Google's *Google Assistant*, *Apple's Siri* and *Microsoft's Cortana* on devices to interact with people in their homes, cars, and jobs. These technologies allow users to interact with a computer or device that interprets what they say and responds to their questions or commands. Each of these assistants has its own unique 'wake word' and processing system. For example, Alexa uses the wake word "**Alexa**", while Siri uses "**Hey Siri**."[3]

[3] SimeononSecurity, 'Securing voice assistants and addressing privacy concerns' available at <https://simeononsecurity.com/articles/securing-voice-assistants-and-addressing-privacy-concerns> last accessed 19 February 2025.

2.3 Many types of voice-activated technology learn language the same way children do.[4] That is, quickly, easily, and without effort or formal teaching. Children who are never spoken to will not acquire language. In other words, children learn based on how other people use language with and around them. Similarly, voice recognition systems must receive language input and be interacted with to learn how to recognize patterns and make connections in human language. Without this input and training, many voice recognition systems likely would not be able to function accurately as they currently do.

2.4 Voice activation technology has revolutionized the way we interact with our devices, making technology more accessible and inclusive for a wider range of users. This transformative feature allows individuals to control devices, access information, and communicate with others simply by using their voice. For people with physical disabilities, voice-activated devices can be life-changing, providing a level of independence that might not be possible otherwise. Similarly, for the elderly or those with visual impairments, voice commands offer a convenient and user-friendly alternative to traditional input methods like keyboards and touchscreens.

2.5 From an inclusivity standpoint, voice activation opens up new avenues for engagement and participation. It breaks down barriers for non-native speakers and those with literacy challenges, as speaking is often more intuitive than typing. Moreover, advancements in natural language processing (NLPs) have made it possible for voice-activated devices to understand a wide range of accents and dialects, further enhancing their accessibility.

3. Types of Voice Activation or Recognition System.[5]

They are of two types:

a. Text Dependent Voice Recognition System

b. Text Independent Voice Recognition System

3.1 Text Dependent Voice Recognition System

These systems require the speaker to say a predetermined word or phrase (known as "Pass Phrase"). This Pass Phrase is then compared to an already captured sample. In

---

4 *Ibid*.

5 Bäckström, Räsänen, and Zewoudie, 'Speaker recognition and Verification' available at <https://speechprocessingbook.aalto.fi/Recognition/Speaker_Recognition_and_Verification> last accessed 19 February, 2025.

text-dependent methods, the speaker verification system has prior knowledge about the text to be spoken and the user is expected to speak this text. Text-dependent systems achieve high speaker verification performance from relatively short utterances.

3.2 Text Independent Voice Recognition System

These systems are trained to recognize a person without a Pass Phrase. They require longer speech inputs from the speaker to identify vocal characteristics. In a text-independent system, the system has no prior knowledge about the text to be spoken and the user is not expected to be cooperative.

4. Advantages of Voice Activation Devices.

Some of the biggest advantages of using voice activation devices include:

a. Improved Access to Information: With voice search capabilities, users can obtain information without the need to read or type. This is particularly beneficial for individuals with visual impairments or reading difficulties.

b. Assistance for the Elderly: As dexterity and vision may decline with age, voice activation can make technology more approachable for older adults, helping them stay connected with loved ones and access entertainment features.

c. Support for Non-Native Language Speakers: Voice-activated devices that support multiple languages can assist non-native speakers in navigating technology and accessing services in their preferred language.

d. Enhanced Mobility and Independence: Voice-activated devices empower individuals with mobility impairments by enabling them to control their environment without physical interaction. For example, smart home devices can adjust lighting, temperature, and even lock doors through voice commands.

e. Learning and Development: Children with learning disabilities can engage with voice-activated educational tools that provide interactive learning experiences tailored to their needs.

An example that highlights the impact and usefulness of voice activation is stories of individuals with cerebral palsy who were able to express themselves and perform tasks

independently using a voice-activated assistant. This technology not only facilitated their daily activities but also provided them with a sense of autonomy and confidence.[6]

Voice activation is more than just a convenience; it is a gateway to a more inclusive world where technology adapts to the needs of its users, rather than the other way around. As this technology continues to evolve, it holds the promise of creating a more equitable and accessible digital landscape for everyone.[7]

5. Disadvantages of using Voice Activated Devices.

Below are the disadvantages and barriers to using voice-activated technology that can affect users' ability to engage with it. Some of the biggest concerns about it include:

a. **Lack of Accuracy and Misinterpretation-** While Voice Recognition Technology recognizes most words in the English language, it still struggles to recognize names and slang words. It also cannot differentiate between homophones such as "their" and "there".[8]

b. **Time, Costs and Productivity-** There is no doubt that technology can speed up a process. However, in the case of the voice recognition system, users may have to invest more time than expected. Users have to review and edit the voice-activation programme to correct errors. Some programs adapt to voice and speech patterns over time which may slow down the workflow until the program is up to speed. Most users also need to learn how to deploy the voice-activation system.

c. **Inaccuracy:** Although the accuracy of voice-activated technology has increased dramatically in the last several years, it still is not perfect. One will likely still encounter some minor inaccuracies or errors when using voice activation.

d. **Limitations:** Voice-activated technology is currently capable of only doing so much. There are limitations to how it can be used, and it will take more time to develop more applications and uses of voice recognition.

e. **Multi-tasking:** The general impression is that using voice recognition helps with multitasking, but it may just be disruptive. For instance, using voice assisted

---

6 Clive Gilbert 'Voice recognition assistants help people with severe speech impairments' available at <https://abilitynet.org.uk/news-blogs/voice-recognition-assistants-help-people-severe-speech-impairments> last accessed 22 February 2025.

7 *Ibid*.

technology can still be a distraction for drivers, especially when it fails to work accurately.

Depending on how a user engages with voice-activated technology and how it is used, the benefits may easily outweigh the drawbacks (or vice versa). It all depends on what type of experience the user wants to have with voice recognition technology.

6. Security and Privacy Concerns with Voice-Activated Devices.

In the realm of interactive technology, voice-activated devices have become ubiquitous, weaving seamlessly into the fabric of our daily lives. From smartphones to smart homes, these devices offer unprecedented convenience, responding to our commands with near human understanding.

However, this convenience comes with a cost because as we invite these devices into our homes, we also open the door to new vulnerabilities where every word could be monitored, and personal data could be at risk. Reports of data breaches and unauthorized listening have surfaced, raising alarms about the extent to which these devices could be exploited by cybercriminals or even used by companies to intrude on our private lives.

6.1 Some Privacy Risks Associated with Voice-Activated Devices:

a. User Consent and Awareness: Many users are not fully aware of the permissions they grant to these devices. The default settings often favour data collection over privacy, and changing these settings can be non-trivial for the average user.

b. Children and Privacy: Voice-activated devices in homes with children pose unique challenges, as children may interact with these devices without an understanding of privacy implications. There have been instances where children place orders for expensive items through voice commands, highlighting the need for better controls.

c. Security Flaws: Devices can have vulnerabilities that hackers could exploit. Researchers from Tokyo and the University of Michigan have demonstrated how a laser pointer could be used to silently command voice-activated devices from a distance, potentially unlocking doors or making online purchases.[9]

[9] Marriella Moon 'Laser can silently issue voice commands to your smart speakers' available at <https://www.engadget.com/2019-11-05-lasers-voice-commands-smart-> last accessed 23rd February 2025.

The researchers explained that there is a small plate called a diaphragm inside a devices' microphone that moves when hit by sound. Lasers can replicate that movement and convert it into electric signals that the device can understand. The research outcome disclosed that opening the garage door by taking over *Google Home* was easy to do, and the researchers could have easily made online purchases, opened doors protected by smart locks and even remotely unlocked cars connected to voice AI-powered devices by using the same method.

1. Legal and Ethical implications: Law enforcement agencies have sought access to recordings from voice-activated devices for criminal investigations. This raises questions about the extent to which these devices can be used to surveil individuals without their consent.
2. Data Collection and Usage: Voice-activated devices are always listening for their wake word, and this means they could potentially record private conversations. Companies assert that recordings are used to improve service quality, but users often lack clarity on where their data ends up or how the data is used. For example, a smart speaker may send recordings to a server for processing, which could be accessed by employees for quality control.
3. Psychological Impact: The presence of always-on devices can alter behaviour, with users becoming more guarded in their conversations, leading to limitations on free speech and expression within one's own home.
4. Third-Party Access: Many voice-activated devices integrate with third-party services, increasing the risk of data exposure. Each additional service represents another point of potential failure, as seen in incidents where private conversations were sent to random contacts due to software glitches.

7. Some Regulatory Frameworks Governing Voice Data Privacy.

Although the proliferation of voice assistants has transformed user interaction with technology, a complex legal framework governs the collection, use, and storage of voice data. This framework is primarily shaped by data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, Canadian Consumer Privacy Protection Act (CCPA) and the Nigerian Data Protection Act in Nigeria (NDPA). These regulations impose stringent

requirements for legal compliance, mandating that organizations obtain explicit user consent before processing voice data.[10]

These regulations aim to mitigate risks associated with data breaches and unauthorized access while promoting accountability among organizations utilizing voice assisted technology. As such, companies must navigate these evolving legal landscapes to ensure adherence to regulatory standards and protect user privacy effectively

Moreover, they require businesses to implement robust security measures to safeguard user information from unauthorized access and breaches. The legal landscape also emphasizes the importance of transparency, compelling companies to disclose how voice data is utilized and stored. As voice technology continues to evolve, ongoing legal scrutiny will likely shape best practices for data protection, ensuring that user rights are upheld in an increasingly digital environment.

8. <u>Best Practices for Users to Safeguard Personal Data on Voice-Activated Devices.[11]</u>

a. **Deleting Voice History and Data Regularly**: Digital assistants store our voice conversations to improve performance and understand user preferences. However, allowing these recordings to be stored in the cloud can pose a risk, especially if unauthorized individuals gain access to them. Regularly deleting your voice records helps reduce the amount of personal data stored by these services.

b. **Managing privacy settings:** Just like every other technology, voice assistants usually come with default privacy settings that may not be in line with our privacy preferences. Therefore, it is essential to review the privacy settings on our voice assistant and configure them to suit our needs. It is pertinent to ensure that we enable features that we use frequently and consider disabling features that pose privacy risks, such as always-on listening. Always-on listening allows voice assistants to listen to our conversations even when we are not actively using them, which can pave the way for a significant privacy concern. If these mitigation

---

[10] Article 7, General Data Protection Regulation, 2016 specified further in recital 32.
California Consumer Privacy Act of 2018 (Cal. Civ. Code §§1798.100 - 1798.199.100)
Section 12(2) of the Canadian Consumer Privacy Protection Act, 2020.
Section 2(1)5, 26, and 30(1) of the Nigerian Data Protection Act 2023.

[11] Best Practices for protecting your privacy when using voice assistants available at <https://digitalwebhelp.com/best-practices-for-protecting-your-privacy-when-using-voice-assistants> last accessed, 23 February 2024.

strategies are implemented, we can significantly improve the voice assistant's privacy and security.

c. **Limit the number of third-party integrations**: Voice assistant companies often integrate with third-party services, such as music streaming platforms, ride-sharing apps, and home automation systems. While these integrations offer additional services and features, they can also pose privacy risks as they share data with third-party companies that are beyond our control. To mitigate privacy risks associated with third-party integrations, it is important to limit the number of integrations used, and reviewing the privacy policies of third-party services accessed through the voice assistant is an added advantage. Alternatively, since some voice assistants allow one to disable third-party integrations entirely, such options can help reduce the risk of data sharing with unknown third-party services.

d. **Use string passwords and Two-Factor Authentication**: Passwords are a first line of defense against unauthorized access to voice assistants and online accounts. For instance, ensuring the use of unique and strong passwords and enabling two-factor authentication (2FA) wherever possible can help add an extra layer of security. Two-factor authentication requires a user to provide two forms of identification, such as a password and a unique code sent to a mobile device, to access an account. This makes it much harder for hackers to gain access to your voice assistant and personal data.

9. Conclusion

While voice-activated devices offer significant benefits, they also bring forth complex security and privacy challenges. Users must navigate these waters with caution, staying informed about the potential risks and actively managing device settings to safeguard personal information.

The reliance on voice-activated technologies raises critical issues related to user consent, as many individuals may not fully understand the extent to which their data is being collected and utilized. Informed consent is often compromised due to insufficient user education regarding data practices.

Furthermore, a lack of data transparency can lead to a diminished sense of control among users. The need for heightened user awareness is crucial; individuals must be equipped

with the knowledge to navigate privacy settings and understand the implications of their interactions with these devices.

For further information on this article and the area of law,
please contact Idorenyin Ekpenyong
at S. P. A. Ajibade & Co., Lagos by
Telephone (+234.1.270.3009; +234.1.460.5091),
Fax (+234 1 4605092)
Mobile (+234.7038229780)
Email: iekpenyong@spaajibade.com
www.spaajibade.com