

Voice Assistants and Biometric Data

Amazon's Violations of Children's Privacy Rights

Themes:

Data Security & Privacy

Prerequisites:

- None for the Case Study section

Owner:

[Center for AI and Data Ethics](#) at University of San Francisco

Author(s):

Hadley Dixon and Robert Clements

Links:

- Github repository: <https://github.com/caidecasestudies/case-study-voice-assistants>
- PDF

License:

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International
[CC BY-NC-SA](#)

Citation:

Dixon, Hadley and Clements, Robert. (2024). <https://github.com/caidecasestudies/case-study-voice-assistants>. Voice Assistants and Biometric Data: Amazon's Violation of Children's Privacy Rights.

DOI:

Objective:

The purpose of this case study is to introduce issues around data privacy and data security by learning the details about a specific lawsuit brought against a popular tech company, and use the details and results of that lawsuit to discuss the potential harms done by this company and other similar companies and gaps in our current laws and regulations around privacy.

Instructions:

1. Read through the case study individually and then answer the discussion questions as a group, or in small groups.

Case Study:

In November 2014, Amazon released the first version of its voice-activated digital assistant, Alexa, along with the Amazon Echo device. Alexa's capabilities have since expanded and has become a prominent player in the digital assistant market alongside Apple's Siri and Google's Home Assistant. These technologies offer a seamless and hands-free way to interact with various devices and bring convenience to daily tasks such as setting reminders, playing music, and browsing the web. The natural language processing capabilities of these voice assistants make them user-friendly and accessible to a broad audience, making this technology essential to the smart-home ecosystem.

The rapid development of voice assistant technology in recent years raises significant privacy concerns due to the inherent need to transmit, store and process voice data for the proper functioning of these devices. Voice data holds crucial information, including the tone, word choice, and frequency of speech. Once stored, voice detection models trained on this data can detect especially intimate details, such as a user's height, weight, ethnicity, personality traits, emotional state, and demeanor ([Winters, 2022](#)). The efficacy of voice assistant technology relies on the ability to store biometric data. The subsequent privacy considerations should address if this data should be stored, for how long, who is able to view stored data and for what purpose. In the absence of limiting its collection, protection of this data becomes crucial, especially regarding safeguards for children.

On May 31st, 2023, the Department of Justice (DOJ) and the Federal Trade Commission (FTC) filed a legal complaint, [USA v. Amazon.com, Inc \(2023\)](#), against Amazon for allegedly violating the Children's Online Privacy Protection Act (COPPA) Rule and for deceptive practices regarding data deletion. The significance of this case extends beyond Amazon itself, serving as a critical examination of AI privacy rights and the responsibility of companies in safeguarding user data, particularly biometric data ([FTC, 2023a](#)).

Congress enacted the [Children's Online Privacy Protection Act \(COPPA\) of 1998](#) to protect the safety and privacy of children online by prohibiting the unauthorized or unnecessary collection of children's personal information by operators of online services. Provisions of COPPA require that an operator of a commercial website or online service directed to children under 13-years-old notify parents about the information they collect from children, obtain parents' consent for the collection of that data, and allow them to delete that information at any time. Additionally, the COPPA

Rule prohibits the retention of information collected from children under 13 for longer than “reasonably necessary” to provide the service. In this context, personal information explicitly refers to a child’s first and last name, an audio file of a child’s voice, and parental information collected from a child’s online account.

According to the complaint Amazon’s virtual assistants include voice activated services aimed at children under 13-years-old, specifically “FreeTime Unlimited on Alexa” and the Echo Dot Kids smart speaker, which offer children’s audiobooks, and audio-based Alexa applications such as voice controlled games, stories, jokes, and educational tools ([FTC, 2023c](#)). More than 800,000 children under 13-years-old have their own Alexa profiles, which include the child’s name, birthdate, gender, and a link to the parent’s profile. The allegations state that Amazon violated data retention policies for children as outlined in COPPA and deceived parents and Alexa users about deletion practices. This follows several instances of parents’ requests to delete their children’s voice data, with Amazon responding by deleting files in some databases while maintaining them in some form elsewhere – meaning the information was available for Amazon to use for its own purposes. Also, important to note is that the original data when initially stored was made available to thousands of employees that had no need for accessing the data and did not work on any Alexa-based teams. The complaint alleges that Amazon prevents parents from exercising their deletion rights under the COPPA rule and kept voice and geolocation data for years, violating the duration of which it is “reasonably necessary” to provide the service. By retaining this data indefinitely and using it to train their algorithms, the plaintiffs claim Amazon has violated COPPA and put children’s data at risk of harm from unnecessary access.

In response, Amazon claimed it retained children’s voice recordings in order to better respond to commands, allow parents to review them, and to improve Alexa’s speech recognition and processing capabilities. The company claims the utility in retaining children’s voice data lies in the differing speech patterns between children and adults, which ultimately provide the company with valuable data when training their voice detection models.

Following the complaint, the proposed court order imposes provisions on Amazon, as well as levying a \$25 million civil penalty. These provisions prohibit Amazon from using geolocation, voice information, and children’s voice information when subject to consumers’ deletion requests and from misrepresenting its privacy policies related to the biometrics of children. Additionally, Amazon is required to delete inactive Alexa accounts of children and implement a privacy program related to the company’s use of geolocation information, which was not formerly in existence. All users must be notified about the complaint filed by the FTC-DOJ, as well as Amazon’s updated data retention and deletion practices.

Discussion Questions:

1. What goals and purposes were involved in the actions taken by the FTC-DOJ?

2. Were the circumstances of Amazon's violations created intentionally, unintentionally, or as a side effect of corporate incentives?
3. How do Amazon's actions put children at risk of harm? In what ways can biometric data be exploited in the hands of an unsanctioned third party?
4. Should there be an equivalent to the COPPA rule for adults or certain sub-populations of adults?

This case is one of many against Amazon ([FTCb, 2023](#)). Users are questioning, to what extent will companies sacrifice privacy for profits? It is important to ensure to users that artificial intelligence (AI) systems are designed with privacy in mind and that individuals maintain ownership over their data.

To address these privacy concerns, it is crucial for companies to implement robust data protection measures. This includes strict adherence to existing regulations, such as COPPA. California, Texas, Washington, and Illinois already have enacted laws pertaining to the collection of voice data. One policy in Illinois requires companies to obtain written consent from individuals before collecting such data, and afterward are prohibited from selling or profiting off of the information, facing financial penalties if violated. Furthermore, there is a need for enhanced oversight and accountability mechanisms. Settlements like the one proposed by the FTC send clear warnings to companies developing AI about the consequences of neglecting user privacy rights. Similarly, regular audits and assessments by regulatory bodies can help ensure compliance, and companies should act proactively to address user requests for data deletion. Proactive efforts become increasingly important when considering interactions between voice assistants and other devices in the home. Vulnerabilities compound when voice data is linked with other sensitive information such as the home's floor plan from robot vacuums, or the use frequency of the home security system. Implementing privacy-by-design principles in the development of AI technologies can also contribute to minimizing the risks associated with data collection and retention.

References:

Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (1998).

Federal Trade Commission (FTC). (2023a, May). FTC and DOJ charge Amazon with violating children's privacy law [Press release]. Retrieved from <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>

Federal Trade Commission (FTC). (2023b, May). FTC says Ring employees illegally surveilled customers, failed to stop hackers from taking control of users' cameras [Press release]. Retrieved from <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users>

Federal Trade Commission (FTC). (2023c, May). Out of the mouths of babes? FTC says Amazon kept kids' Alexa voice data forever – even after parents ordered deletion [Blog post]. Retrieved from <https://www.ftc.gov/business-guidance/blog/2023/05/out-mouths-babes-ftc-says-amazon-kept-kids-alexa-voice-data-forever-even-after-parents-ordered>

United States of America v. Amazon.com, Inc, Case No. 2:23-cv-00811 (United States District Court Western District of Washington 2023). Complaint for Permanent Injunction, Civil Penalties, and Other Relief. Retrieved from https://www.ftc.gov/system/files/ftc_gov/pdf/Amazon-Complaint-%28Dkt.1%29.pdf

Winters, M. (2022, January 20). Collection of voice data for profit raises privacy fears. ABC News. Retrieved from <https://abcnews.go.com/Technology/collection-voice-data-profit-raises-privacy-fears/story?id=96363792>