"Alexa, Delete My Child's Data" – Amazon Agrees to Pay $25 Million for Online Privacy Violations

On May 31, 2023, Amazon agreed to pay a $25 million civil penalty to settle Federal Trade Commission (FTC) charges that the company retained sensitive information collected from children using Alexa, in violation of the Children's Online Privacy Protection Act (COPPA). Alexa is Amazon's voice assistant service, which collects and retains vast amounts of data from voice recordings to geolocations.

Under COPPA, it is "unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child" without providing notice at the time of collection and obtaining veritable consent from a parent or guardian. The Act is intended to protect the safety and privacy of children under 13 years of age while using the internet for various activities.

The complaint, filed by the Department of Justice (DOJ) on behalf of the FTC, alleges three ways in which Amazon violated COPPA:

1) Alexa was programmed to keep children's recordings indefinitely to improve its Alexa algorithm, whereas COPPA states that personal information collected online from a child should be retained "for only as long as is reasonably necessary to fulfill the purpose for which the information was collected."
2) Amazon did not give parents adequate notice of the ability to have their children's personal information deleted, and COPPA expressly states that the operator is required to "provide notice and obtain verifiable consent prior to collecting, using, or disclosing personal information from children."
3) Amazon retained transcripts of children's voice recordings even when parents instructed Amazon to delete the files, thus violating COPPA, which states that parents should have the ability to refuse to permit the operator's future online collection of personal information from the child and to direct the operator to delete the child's personal information.

The FTC alleged that Amazon knew of these privacy issues and failed to fix them, as well as falsely assured its users that they could delete their data collected from Alexa. In addition to the $25 million penalty, Amazon is now required to delete inactive Alexa child accounts, children's voice recordings and geolocation data. Amazon must now notify its users of retention and deletion practices and about the FTC-DOJ action against them. The company is prohibited from misrepresenting its privacy policies and must create and implement a privacy program related to its use of geolocation information.

This is not the first time that Amazon has faced privacy concerns. In 2018, Amazon acquired Ring, the home security camera service. In a separate case, the FTC alleged that Ring committed "egregious violations" of users' privacy in which employees had unrestricted access to customers' videos and hackers were able to hijack various accounts. Ring's questionable security and privacy practices spanned from 2016 through 2020, and Amazon agreed to pay $5.8 million to settle these claims.

Key Takeaways

The FTC continues to closely monitor children's privacy concerns. Social media networks, video game services and electronic device manufacturers will continue to be subject to increased regulatory scrutiny amid public concerns regarding how these companies treat young consumers. Companies should remember the following tips:

- Voice recordings and associated transcriptions must be treated as sensitive information. This type of data is known to "raise significant consumer privacy and data security concerns" as indicated in the FTC's May 2023 Policy Statement on Biometric Information.
- COPPA's jurisdictional scope is broad and its requirements for notice and collection apply across a wide range of industries. The onus is on businesses to monitor compliance and promptly delete data that is no longer "necessary to fulfill the purpose for which [it] was collected."
- At least annually, review your company's privacy practices to ensure compliance with all public-facing privacy disclosures. Disclaimers and promises for privacy protection are meaningless when the data is being using for unauthorized purposes. Failure to adhere to these representations may result in regulatory actions and fines.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including compliance with COPPA and other privacy authorities. If you have any questions about COPPA or FTC privacy enforcement, please contact an attorney in Bond's cybersecurity and data privacy practice.

Special thanks to Summer Law Clerk Jéla Paul *for her assistance in the preparation of this memo.*

BOND SCHOENECK & KING ATTORNEYS