Published on *The National Law Review* https://natlawreview.com

Connected Toys Scrutinized Over Privacy and Security Weaknesses

Article By:

Data Privacy & Cybersecurity

Two connected toys, My Friend Cayla and i-Que robot, by Genesis have been receiving trans-Atlantic attention this month for alleged privacy, security and advertising law violations. On December 6, 2016, public interest organizations in the U.S. and European Union submitted complaints to the Federal Trade Commission ("FTC") and EU Data Protection Authorities ("DPAs"). The complaints describe a number of privacy and security weaknesses in the toys, such as the toys failing to obtain consent from parents for the processing of minors' personal data, and weak security safeguards that allow the toys to be easily hacked.

The Toys

The toys provide children with an interactive experience via a microphone, speech recognition software, connection to the Internet, and speakers. Such toys have become very popular because they are constantly learning from these interactions through the speech recognition software and Wi-Fi or Bluetooth connection to the Internet (which is able to search Google, Weather Underground and Wikipedia). The toys are able to talk to children, make jokes, play games, and much more. While kids play with the toys, much of the interactions are recorded and then shared with other parties.

The Complaints

Specifically, the U.S. FTC complaint alleged violations of the Children's Online Privacy Protection Act ("COPPA") and consumer protection law, and was filed by the Electronic Privacy Information Center ("EPIC"), the Center for Digital Democracy ("CDD"), Consumers Union and the Campaign for a Commercial Free Childhood ("CCFD"). Under COPPA, operators of websites or online services directed at children under 13 years of age must post their privacy policies, and notify parents of their data collection practices and receive verifiable parental consent before collecting personal data from children.

The EU complaint alleges the toys violate the EU Data Protection Directive and EU Unfair Contract Terms Directive, and was filed with EU Commission, the International Consumer Protection and Enforcement Network, and national DPAs in Norway, Greece, Belgium, France, the Netherlands and Ireland. Under current EU law and the upcoming General Data Protection Regulation ("GDPR"), data controllers and processors must meet certain obligations when they collect, process, and share data.

Next Step

As everyday items are becoming a part of the Internet of Things (“IoT”), more and more companies will need to consider data privacy and cybersecurity as part of their designs. In general companies should take into account state, federal, and international data protection laws when designing their products and services. Most laws have certain requirements that must be met for companies to lawfully collect, process and share data. An effective way to understand the potential privacy and security issues of your company’s products and services is to map the company’s data flows, and to conduct a privacy impact assessment and testing of security vulnerabilities. In addition, as shown by the recent complaints in the EU and U.S., toy manufacturers must be sensitive to children’s privacy and security.

National Law Review, Volumess VI, Number 354