LORMAN

Regulating the Internet of Toys

Prepared by:
Amy C. Pimentel
McDermott Will & Emery

Published on www.lorman.com - March 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Regulating the Internet of Toys

Written by Amy C. Pimentel 7/28/17

New technologies and the expansion of the Internet of Things have allowed children of this generation to experience seamless interactive technologies through microphones, GPS devices, speech recognition, sensors, cameras and other technological capabilities. These advancements create new markets for entertainment and education alike and, in the process, collect endless amounts of data from children–from their names and locations to their likes/dislikes and innermost thoughts.

The collection of data through this Internet of Toys is on the tongues of regulators and law enforcement, who are warning parents to be wary when purchasing internet-connected toys and other devices for children. These warnings also extend to connected toy makers, urging companies to comply with children's privacy rules and signaling that focused enforcement is forthcoming.

Federal Trade Commission Makes Clear That Connected Toy Makers Must Comply with COPPA

On June 21 2017, the Federal Trade Commission (FTC) updated its guidance for companies required to comply with the Children's Online Privacy and Protection Act (COPPA) to ensure those companies implement key protections with respect to Internet-connected toys and associated services. While the FTC's Six Step Compliance Plan for

COPPA compliance is not entirely new, there are a few key updates that reflect developments in the Internet of Toys marketplace.

1. The Compliance Plan clarifies that any company providing "connected toys or other Internet of Things devices" are covered by COPPA, identifying a number of examples including "mobile apps that send or receive information online (like network-connected games, social networking apps or apps that deliver behaviorally-targeted ads); internet-enabled gaming platforms; plug-ins; advertising networks; internet-enabled location-based services"; and under certain conditions, voice-over internet protocol services.

2. The revised Compliance Plan discusses two newly-approved methods for getting parental consent: (a) asking knowledge-based authentication questions and (b) using facial recognition to get a match with verified photo identification. Obtaining a parent's permission before collecting personal information online from children under has always been a key component of COPPA; however, these new methods seek to ease this burden by blessing these two additional ways for companies to comply with the consent requirements.

3. The Compliance Plan reiterates that as technologies evolve, companies have new ways of collecting data, some of which may affect obligations under COPPA. As companies' business plans change, the FTC urges them to think about how their data collection might affect the privacy of children.

Federal Bureau of Investigation Cautions Consumers of Privacy and Security Risks

On July 17, 2017, the Federal Bureau of Investigation (FBI) released a Consumer Notice that encouraged consumers to "consider cyber security prior to introducing smart, interactive, Internet-connected toys into their homes or trusted environments." The FBI warns that the exposure of the child's personal information collected through these toys could create opportunity for child identity fraud and misuse of sensitive data, such as GPS location information, visual identifiers and known interests that could "garner trust from a child" and "present exploitation risks." The FBI also encouraged all consumers to research areas and circumstances concerning the toys and online services where laws may or may not provide coverage, highlighting consumer laws that protect children, such as COPPA and Section 5(a) of the FTC Act, which prohibits unfair and deceptive practices in the marketplace.

The FBI lists several recommendations for consumers to consider prior to using Internet-connected toys, which include:

- Connecting toys only in environments with trusted and secured Wi-Fi Internet access;
- Researching reported security issues, the toy's Internet and device connection security measures and the company's reputation and posture for cyber security;
- Using strong and unique login passwords when creating user accounts;

- Reviewing the user agreement disclosures and privacy practices of the toy company, noting how companies will notify of a cyberattack, vulnerability or change in practices; and

- Providing only what is minimally required when inputting information for user accounts.

Keeping up with Technology and Regulation

There are both positive and negative aspects to consider as the Internet of Toys continues to evolve. Technological developments create new ways of learning and interacting, but can pose security and privacy risks to children. While there are several steps consumers can take to protect themselves against these risks, regulators and law enforcement are putting a burden on toy makers to use a higher standard of safety and protect the privacy of children. The future for the Internet of Toys is promising, but connected toy makers should make concerted efforts to build trust with parents and children by taking privacy-conscious steps, such as (a) developing a clear and concise privacy statement that allows parents to make an informed choice about using your product; (b) investing in developing creative and intuitive ways to notify parents and children when information is being collected through the toy; and (3) establishing strong data security practices, such as using encryption, double factor authentication and requiring the use of complex password. Industry leaders that follow these and other privacy and security best practices will be well suited to succeed in this growing market.