DATA PRIVACY AND CYBERSECURITY

THE INTERNET OF TOYS: LEGAL AND PRIVACY ISSUES WITH CONNECTED TOYS

by Sara H. Jodka

Most people have heard of the Internet of Things, or IoT. With the holidays fast approaching, and with the onslaught of new smart and Internet-connected smart toys, for parents and toy manufacturers, at least for the next few weeks "IoT" means the Internet of Toys.

Smart toys first sparked interest in 2015 when Hello Barbie a connected-smart doll was introduced. Hello Barbie came equipped with a microphone, voice recognition software and artificial intelligence that allowed a call-and-response function between the child user and the doll (think how Siri works). The backlash and hacking concerns loomed so large Hello Barbie got its own Twitter hashtag, #HellNoBarbie.

Since 2015 the technology and legal implications regarding these types of toys has only grown as the market now includes smart toys, such as Talk-to-Me Mikey, SmartToy Monkey, and Kidizoon Smartwatch DX; connected toys, such as SelfieMic and Grush; and other connected smart toys such as Cognitoys' DINO, and My Friend Cayla. There is also a new crop of GPS-enabled wearables marketed as allowing parents to monitor and track their child's movements, including Kidizoom Smartwatch DX, a smart toy. For those keeping track, that's three separate types of toys: (1) smart toys; (2) connected toys; and (3) connected smart toys.

There are many reasons why these toys/wearables are problematic and the privacy issues for each are analyzed differently based on functionality. Some that function like the Amazon Echo, and unlike Smartphones, are *always on*, and blend into the background of their users' daily lives. They also collect a significant amount of personal information, some of it legally-protected, especially in the context of information about children and/or from children. Many are so sophisticated they are able to adapt to a child user's actions and process information from many sensors through the use of microphones, voice sensors, cameras, compasses, gyroscopes, radio transmitters, or Bluetooth. Connected toys connect to the Internet, which allows remote servers to collect data to power the toy's intelligence functionality.

The other ever-developing aspect of this technology is that the technology has expanded outside the home to schools, to assist with educational functions, and to health care settings, to help stabilize child/patients emotions or to manage anxiety.

With all that background, the next issue is, where is the law? There are a number of issues to consider when discussing smart toys marketed to and used by children: the Children's Online Privacy Protection Act (COPPA) and Federal Trade Commission (FTC) enforcement, the Family Educational Rights and Privacy Act (FERPA), the Health Information Portability and Accountability Act (HIPAA), state consent laws, constant connection, and, of course, privacy. Here is how it breaks down.

COPPA / FTC Enforcement

Of the three types of toys, connected toys are the most problematic as they present the greatest social and legal concerns. For starters, they can connect to Internet-based platforms and to other devices enabling data gathering, processing and sharing. They also can connect to each other and to the Internet through various means, WiFi routers, cellular data networks, and Bluetooth. There are four types of connected toys: Toys to Life, Robotics (e.g., WowWee's CHiP robotic dog and Sphero Star Wars BB-I companion robot), Wearables, and Learning Development Toys. Given the dangers, connected toys are the ones that trigger a number of U.S. privacy laws, including COPPA, which is the primary privacy law governing these toys.

Section 5 of the Federal Trade Commission Act directs the FTC to protect consumers from "unfair or deceptive acts or practices in or affecting commerce." This puts COPPA in the FTC's enforcement crosshairs.

COPPA applies to online services providers, *i.e.*, websites, directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child.

The definition of "personal information" under COPPA is quite broad and includes: names; addresses; online contact information; screen or user names; telephone numbers; Social Security numbers; persistent identifiers that can be used to recognize a user over time across different websites or online services; geo-location; and photographs, video, or audio containing the child's image or voice.

COPPA is designed to protect children under the age of 13 from certain online activity. The high level view of COPPA has five main components:

1. **Notice of Data Practices.** This requires operators give direct notice to parents of its data collection practices. Certain statements are also required, including how consent is to be given, and that no personal information of a child will be collected, used or disclosed without parental consent. The operator also has to reveal the personal information that will be collected and link their privacy policy.

2. **Parental Consent (Verified).** Verifiable parental consent must be given before an operator can collect personal information from a child. The consent has to take into account available technology and can include: (a) asking parents to sign and mail a hard-copy consent form; (b) allowing parents to use an online payment system to provide notification of each transaction to the primary account holder; (c) having parents provide consent via phone or video; or (d) checking government-issued identification.

3. **No Conditional Participation.** Operators cannot condition a child being allowed to play a game or being allowed to win a prize on the child disclosing more personal information than "reasonably necessary" to participate in the game, prize, etc.

4. **Required Reasonable Security.** Operators are also required to have and maintain reasonable security procedures to "protect the confidentiality, security, and integrity of the personal information collected from children." If any of the information is transferred to a third party, the operator must ensure the third party has taken similar steps to protect the protected data. *See* COPPA Rule in 2013.

5. **Data Collection.** Operators can only keep personal information collected online from a child as long as reasonably necessary to fulfil the purpose for which it was collected for. When the personal information is no longer needed, the data must be deleted through reasonable measures.

Due to COPPA's requirements, any smart or connected toy that collects personal information from a child could trigger COPPA's requirements. COPPA fines range from $16,000 to $40,000 per violation though the FTC has not taken any action against a connected toy operator. . .yet.

The issues as to how toy manufacturers technically comply with COPPA given the functionality of the toys are complicated. For example, some smart toys will not need parental permission if there is no collection of personal information. Non-personal data that would *not* trigger COPPA would include achievement levels in games, a user's keypress responses, etc. Parental consent would also not be required for connected toys that collect and use a persistent identifier, which would include information such as an IP address or toy/device ID. The exception would apply if the persistent identifier is used to support the internal operation of the service being provided, such as in maintaining/analyzing the service, personalizing content, and performing network communications. Toys that align with these functions with a persistent identifier can be provided to the child user "out of the box," meaning without any registration process that might include parental consent and disclosures.

Other connected toys also work out of the box, but allow for additional features that *would* require consent and proper disclosures as they would be asking for non-personal and personal information that would trigger COPPA, and only allow for the additional functionality once COPPA requirements are met.

On October 23, 2017, the FTC attempted to address some of the issues with connected toys and released its Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings. The release, however, was limited and only addressed the collection of and use of voice recordings and provided:

> The FTC will not take an enforcement action against an operator for not obtaining parental consent before collecting the audio file with a child's voice when it is collected solely as a replacement of written words, such as to perform a search or to fulfill a verbal instruction or request – as long as it is held for a brief time and only for that purpose.

The FTC noted the policy would not apply in cases where an operator requested information via voice that would otherwise be considered personal information, such as a name. In addition, an operator is still required to provide clear notice of its deletion and privacy policies, and of its collection and use of audio files. An operator is also prohibited from making any other use of an audio file before it is destroyed. Lastly, the policy does not affect the operator's COPPA compliance requirements in any other way. As such, the FTC's new guidance is extremely limited, but it does provide manufacturers and operators some relief regarding enforcement.

State Consent Laws

The issues with IoT toys transcend COPPA. One issue with toys that record audio and those that have interaction functionality, meaning the child asks the toy a question and it responds with an answer (think Siri or GoogleNow).

One issue with recording is that there are state law issues (which our HR blog addressed here). In the United States there are two different types of laws governing recording. One-party consent states, which only require consent of one of the parties to the conversation being recorded, and all-party consent states, which require the consent of everybody involved in a conversation before the conversation can be recorded. One-party consent states make up the majority. There are only eleven all-party consent states: California, Florida, Illinois, Maryland, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington.

The consent requirements in all-party consent states are triggered when the owner of the toy submits a voice recording and, to the extent, the child plays with another child and that child's voice is recorded, consent would be required from that child as well. The issue then becomes, how do manufacturers or operators obtain the required consent in these states?

Privacy

The overarching issue to all of this is child privacy. There have been a number of cases where connected toy manufacturers failed to ensure the security of the information they collected. Take for instance the 2015 matter where VTech Electronics North America, LLC (VTech), a company that sold connected tablets marketing for children, suffered a breach that exposed the personal protected data of over 6 million children and 4 million adults, including their names, genders, dates of birth, and, worse, photographs.

Child information is particularly susceptible because they are largely a blank canvas that can be fraudulently used for a long period of time without detection as most parents do not actively monitor their children's information.

In September 2017 the FBI got involved and warned parents their children's new internet-connected toy could be secretly spying on them. Specifically, the FBI warned:

> These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS options.

The FBI's release went on:

> The potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks". The FBI further encouraged consumers to consider "cyber security" prior to introducing smart, interactive, internet-connected toys into their homes …

The GPS functionality in some toys is especially disconcerting because, if breached, it could allow a hacker to know the exact location of a child or to access privately-recorded conversations. This was an issue in February 2017 when Germany banned My Friend Cayla, a smart doll. Germany's telecomm regulator found that the toy could be hacked to record private conversations that were transmitted via the toy's Bluetooth connection.

The Electronic Privacy Information Center, which is known as a U.S. privacy watchdog, also got involved with My Friend Cayla toy and sent a complaint to the FTC regarding the toy's security risks. While the doll has not been banned in the United States, the findings of a congressional inquiry were that the toy indeed recorded private conversations of children 12 and under without parental consent and in violation of COPPA.

Another issue surfaced with CloudPets, a connected stuffed animal that was marketed as allowing parents and their children to exchange cute messages through the toy. While cute in theory, in reality the manufacturer was storing the personal account information and voice recordings online, and in an easily-hackable database. The result was that approximately two million personal recordings from the CloudPets were leaked.

Constant Connection

The constant connection issue also poses privacy threats and new vulnerabilities, which are similar to those concerning related devices such as Amazon's Echo and Google Home; however, these issues are heightened because the user is usually a child.

Amazon Echo and Google Home, and other devices that had Alexa and Google Assistant, however, took steps to protect users, and it would seem that toy manufacturers could take similar steps. In those devices, while the microphone to the device is always on, the devices do not start recording until specific words, referred to as "Wake Words" are said, such as "Alexa" or "OK Google". Once recorded, the recordings are stored in the cloud. Users can review their requests through app/device settings and delete them through the "Setting > History" function (in Amazon) or mass purge via "Your Devices > Echo Dot > Manage voice records." In Google Assistant, it is a function through myactivity.google.com. For more information, check out this Wired article.

Expanding the notion of constant connection and the imagination just ever so slightly forward, it is easy to foresee a situation where a child's toy is subpoenaed or seized pursuant to a search warrant because it possibly recorded relevant evidence.

Takeaways:

As usual, the law is behind the technology. While some old laws may apply to some of these issues, most instances are a new frontier. This means that manufacturers have to think proactively and protect consumers from potential issues related to their technology-based products. It also means that parents buying these toys for their children should be aware that these issues are not fully taken care of and they should remain hypervigilant in reviewing the toys they buy and actively monitoring their children's activities and communications with the toys. This may mean playing with the toy in advance and learning its settings and security features to ensure safe use.

Toys warranting additional scrutiny include, toys that connect directly to the Internet via WiFi; toys that connect via Bluetooth to a device that is connected to the Internet; toys that contain speakers, microphones, recording devices, cameras, wireless transmitters and receivers; toys that have GPS capability or speech recognition capability; toys that connect to a mobile app; toys that request information, such as a name, address, date of birth of other personal information when registering; toys that store information internally; toys that have cloud connection functions; toys that remain connected to the cloud even when they are turned "off".

Here are other tips:

1. **Look for the seal!** The FTC has a certification program that allows manufacturers to get a seal to put on their packaging or website if their toy has been reviewed and found in compliance with children privacy requirements, including KidSAFE.

2. **Research.** Before buying a connected toy, conduct online research to determine if there have been negative reports concerning privacy or other issues with the toy.

3. **Read the fine print.** Manufacturers have to issue certain disclosures regarding the collection, retention, and use of collected information. It is important to read these disclosures, even though they can be quite boring, because they will (or should) tell you what information is collected, where it is stored, whether it is provided to third-parties, and what they can or will do with the collective information.

4. **Use securely.** Just as you would with an online purchase, only use toys when you can verify that the connection is through a secure WiFi connection. While this may mean that your child

cannot use the toy in a restaurant that has an open WiFi, the easy alternative is to provide the child a secure hotspot through your own smartphone and lock down the transfer of data.

5. **Require PINs.** If the toy is Bluetooth-connected, ensure it requires the use of PINs or passwords before pairing with connected devices.

6. **Encryption is always a good idea.** If the toy transmits data to a WiFi access point, a server or the cloud, make sure the transfer is encrypted, meaning the information would be unreadable without the encryption key.

7. **Patch.** If the toy can receive software updates or patches, ensure that toy is kept up to date with such updates or patches. However, prior to installing a patch or update, research to ensure there are no issues with the actual update or patch.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of data privacy and cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.