KIDS & THE CONNECTED HOME: PRIVACY IN THE AGE OF CONNECTED DOLLS, TALKING DINOSAURS, AND BATTLING ROBOTS

DECEMBER 2016

FUTURE OF PRIVACY FORUM

Family Online Safety Institute

Acknowledgements

Future of Privacy Forum (FPF) and Family Online Safety Institute (FOSI) would like to thank the participants and attendees of “Kids and the Connected Home” (July 20, 2016), as well as the following individuals who contributed to the research and analysis in this paper:

Carolina Alonso, Legal & Policy Fellow, Future of Privacy Forum
Stacey Gray, Policy Counsel, Future of Privacy Forum
Emma Morris, Global Policy Manager, Family Online Safety Institute
Jennifer Hanley, Director, Legal & Policy Family Online Safety Institute
Steven Anderson, Legal Intern, Future of Privacy Forum
Hengyi Jiang, Legal Intern, Future of Privacy Forum
Emily S. Tabatabai, Of Counsel, Orrick Herrington & Sutcliffe

TABLE OF CONTENTS

Executive Summary

Connected home ("Smart Home") technologies provide families with an array of benefits, including convenience, customization, and safety. In addition, more parents today are choosing **connected toys** for their children, either for play or for learning and development. Toys popular in the current market connect to each other and to online platforms via Wi-Fi, Bluetooth, or other methods to provide personalized or interactive experiences for children.

While the potential benefits are considerable and include new opportunities for personalized and interactive play and learning, concerns are being raised about whether such "smart" toys are collecting too much personal information from children, as well as how that information may be used or shared, and whether it is secure. As connected toys become more popular and issues of cybersecurity rise in urgency, it is important for key privacy issues to be addressed.

For toymakers and industry professionals, these concerns are particularly critical because toys are used inside the most traditionally private location, the home, and may collect data from children. Trust is a crucial precondition for widespread adoption of connected toys. Parents must be satisfied that the digital products they invite into their homes will safeguard children's privacy and keep information secure.

On July 20, 2016, the Future of Privacy Forum (FPF), the Family Online Safety Institute (FOSI), and Christian Science Monitor Passcode hosted Kids & the Connected Home in Washington, DC. This event featured discussion by a diverse group of industry experts, including: Future of Privacy Forum CEO Jules Polonetsky; Family Online Safety Institute CEO Stephen Balkam; former Federal Trade Commissioner and current Hogan Lovells Co-Leader of Privacy and Cybersecurity Julie Brill; Elemental Path CEO Donald Coolidge; Director of the Atlantic Council Cyber Statecraft Initiative Josh Corman; Passcode Editor Michael B. Farrell; ESRB Privacy Certified Vice President Dona Fraser; and University of Washington Tech Policy Lab Program Director Emily McReynolds.[1]

In this white paper, we discuss and expand upon the issues raised at that event, which concerned the emergence of connected toys and their social and legal implications. In particular, we address the following questions that animate discussions around children and the connected home:

- **Connected Toys.** Does the Children's Online Privacy Protection Act (COPPA) apply to connected toys? And does the screen-less nature of many connected toys suggest that an update to COPPA may be required to adequately address privacy concerns?
- **Connected Homes**. Does COPPA apply to general home devices that serve families?
- **Parental Controls.** Do parents have appropriate controls and information to make informed decisions regarding their children's interactions with the connected home and toys? If not, how can this be addressed?
- **Data Security**. How do we ensure that connected toys are sufficiently secure?

In Part I, we describe the current landscape of connected toys, identifying what distinguishes them from conventional toys and other smart toys. Part II analyzes the existing regulations under the Children's Online Privacy Protection Act (COPPA) that have established important safeguards for information collected from children, and how those regulations apply.

Finally, we discuss leading privacy and security practices that can help parents make informed choices (Part III). Connected toys are still relatively new, and present unique challenges for privacy and security. Toy providers should aim to provide clear privacy notices, including at the point of sale where appropriate; integrate flexible and creative forms of notice into toy design; and ensure meaningful choice mechanisms. Companies should be especially cognizant of the importance of implementing strong security measures to safeguard children's data against unauthorized access or use. While many are increasingly understanding the necessity of building privacy and security into the design of their products, much more can be done to build trust.

I. The Landscape: Connected Toys Are Increasingly Popular and Often Use Children's Data to Enable Interactive Play

Parents and children are seeking new ways to interact during play, and connected toys are becoming a significant and growing part of the children's entertainment market.[2] Connected toys use data and Internet access to provide opportunities for children to play, interact with others, and learn skills.

In this Part, we describe the landscape of modern connected toys, including how they are different from conventional toys and other forms of smart toys. To the extent possible, we also describe the data collected and used by many of these toys. All of the connected or smart toys mentioned and discussed in this paper are described with citations in Appendix I.

Connected Toys Differ from Other Toys Because They Collect, Use, and Share Data Via the Internet

The world of children's toys has come a long way from the days of the familiar teddy bears and dolls of past generations. Modern toys are increasingly equipped with an array of sensors and other sophisticated technology.

Toys integrating technology is nothing new—toys have a long history of incorporating advanced features, including microchips that enable interactivity and engagement. We are all familiar with pull-string dolls that speak, remote controlled racecars, and other such classic toys equipped with electronic or mechanical features. As technology has advanced, we have seen such toys as the generation-defining Tamagotchi (BanDai),[3] and toys like the Sony AIBO, the popular robotic dog first introduced almost 20 years ago.[4] See Fig. 1.

Fig. 1. When Sony's AIBO was first released in 1999, it included a 64-bit processor, 16MB of RAM, and an array of sensors for creating the robot's personality.

Today's world of tech-enabled toys is different in two key respects:

First, advances in computer processing are enabling "smart toys" to interact in more sophisticated ways, even going so far as to simulate intelligence. Smart toys, or toys that contain embedded electronic features such that they can adapt to the actions of the user, can today process more information from a greater variety of sensors. This may include the use of microphones for speech recognition,[5] cameras for detection of patterns and visual cues, accelerometers, proximity sensors, gyroscopes, compasses, radio transmitters, or Bluetooth for communicating between various parts to the same toy. For example, the Playmates Toy Talk-to-Me Mikey uses speech recognition processing to allow the toy to respond with answers to specific questions. See Fig 2.

Fig. 2. Talk-to-Me Mikey is an example of a Smart Toy that is not "connected."

Second, many of today's toys are designed to connect to the Internet, and therefore to remote servers that collect data and power the toy's intelligence. Cloud-based processing can enable sophisticated real-time interactions with toys, including speech recognition that improves over time to adapt to accents and context. Here, we refer to such toys as "**connected toys**."

The distinction between smart toys and connected toys is important: a toy can be very *smart*, but not connected (e.g. a self-contained interactive action figure), and a connected toy can be either smart or not smart. We note that the smartest of the smart toys today are using powerful processing that benefits from cloud-based services.[6]

The most practical reason for drawing this line is that whether or not a toy is connected to the

Internet is a key factor in determining whether or not key U.S. privacy law applies (see Part II for our analysis of COPPA).

More fundamentally, we analyze the privacy issues differently for each. Smart toys that do not connect to the Internet may raise important issues about child development and learning, but because data is not sent remotely, their privacy and security implications are more limited. See Part III (briefly discussing the privacy implications of non-connected toys).

Connected toys, in contrast, can connect to Internet-based platforms or to other devices to enable data collection, processing, or sharing through a computer server. This key feature is what primarily generates concerns today over privacy and data security, and makes them subject to COPPA. See Part II.

Each connected toy on the market today is unique in its data-processing capabilities. Connected toys need not be smart—for example, toys like SelfieMic or the Grush collect and process large amounts of data, but do not incorporate elements of artificial intelligence. See App. I.

This paper primarily focuses on **connected toys**, as they present the greatest social and legal implications with respect to privacy and security. As the market for connected toys continues to grow, it is vital that companies address these issues in a way that instills confidence and trust.

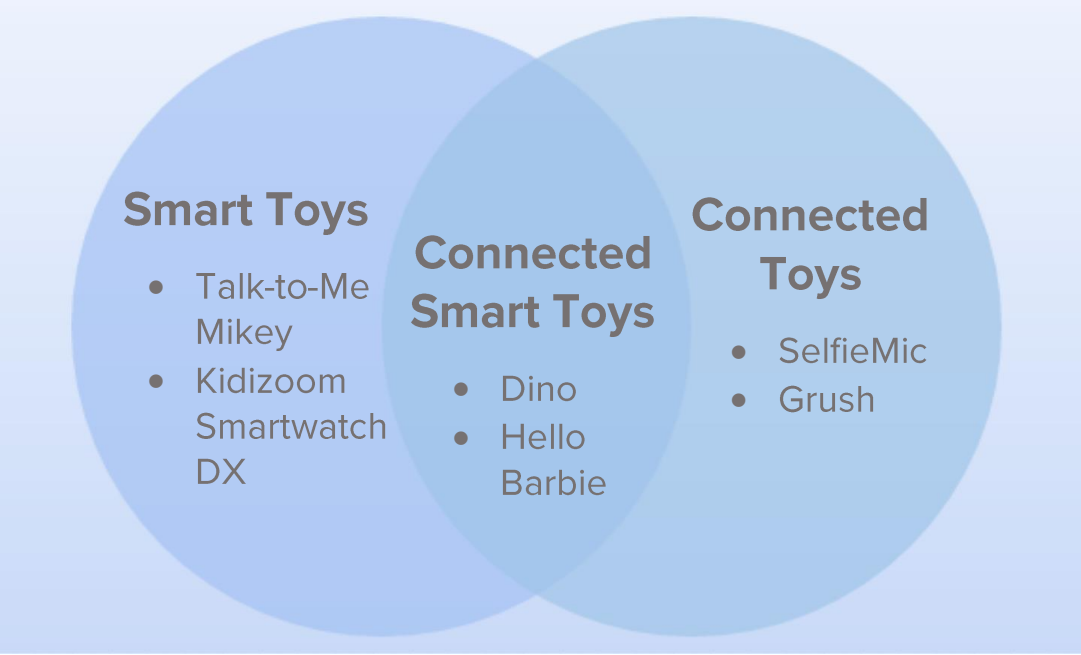


Fig. 3. This Diagram illustrates the distinction between smart toys, connected toys, and connected smart toys. For more details on specific toys, *see* Appendix I.

Connected Toys Use a Variety of Technical Methods to Connect to Online Platforms or Servers

Like many smart home devices, connected toys may connect to each other or to the Internet by an expanding variety of methods, including but not limited to the following examples.

Wi-Fi Routers. Many connected toys require an Internet connection to function, and therefore prompt users to connect to the surrounding Wi-Fi. Data can then be transmitted directly from the toy to a remote server, typically at a data center, where the data is stored or processed, often prompting a return signal to generate an appropriate response in the toy.

For example, Mattel's Hello Barbie connects to Wi-Fi after it is initially set up via its associated app, permitting the doll to communicate directly with a server. This allows the doll to transmit audio files, which are processed remotely for speech-to-text recognition, and to receive a signal in return to respond appropriately to a child's question or comment in a way that simulates a real conversation.

Cellular Data Networks. Some toys may be capable of connecting to the Internet using cellular telecommunications networks (such as 3G, 4G, and LTE), either independently or via an accompanying app. Toys that use cellular networks are still connecting to the Internet—and thus may not differ in their legal implications, *see* Part II—but may interact with different user settings.

Bluetooth Low-Energy. Other toys access the Internet indirectly by connecting first to a smartphone or tablet via Bluetooth Low-Energy (Bluetooth). For example, Connected Furby and Love2Learn Elmo connect to the Internet exclusively through a Bluetooth connection with their associated app on a smartphone or tablet. The Bluetooth connection allows the app to collect data from the physical toy and also from the user's interactions with the app itself. The app then connects to a Wi-Fi or cellular network and sends data to a server where it can be further processed or stored.

In the future, more toys and home devices may integrate sophisticated processing that is done locally, i.e. without transmitting data from the device. However, if data is not sent remotely to outside parties, the implications of such devices are more likely to be security-related and sociological.[7] See Part III.

The Spectrum of Connected Toys Includes "Toys to Life," Robotics, Wearables, Learning Development Toys, and Many More

Connected toys come in every shape, size, and design—from talking dolls, to robots, to location-aware paintball helmets. Broadly speaking, toy industry analysts identify at least four main types of connected toys available on the market today: **Toys to Life, Robotics, Wearables,** and **Learning Development Toys.** These different types of toys can be used in various ways by children, and may collect different kinds and quantities of data. Although not always dispositive, these factors should be considered when designing the appropriate default notice and choice settings in each case.

Toys to Life are a genre of connected toys that involve physical figures or characters that become a child's interactive companions, often by interacting with video games.[8] The toy is often an action figure or a doll with a pre-determined personality, such as Mattel's Hello Barbie. Although it may be interactive on its own, some Toys to Life also become digital characters, such as Edwin the Duck, a physical rubber duck that also becomes a digital, animated companion in its accompanying app.

Fig. 4. Playmation (Disney) is an example of a connected Toys to Life toy.

Disney's Playmation includes physical action figures that connect to wearable armbands and an accompanying app. Children receive "missions" and the action figures begin speaking and become part of the game. Thus, Playmation incorporates elements of Wearable technology, discussed below. Like many connected toys, its functionality expands with the use of an app, which allows children to save their settings and accomplishments.

Often, a Toys to Life toy only requires an app for initial set-up. For example, Mattel's Hello Barbie requires initial set-up via the app in order to obtain the necessary parental consent and connect to a Wi-Fi network. After being set up, the Hello Barbie interacts independently with the child, with no need for the app. Parents have access to their child's personal information through a separate, online account.

Robotics includes toys that are remotely controllable, often with a handheld controller, an accompanying app, or via spoken commands. By far the most popular and fastest-growing category of connected toys,[9] robotic toys include WowWee's CHiP robotic dog and Sphero Star Wars BB-8 companion robot.

Fig. 5. CHiP (WowWee) is an example of a robotic toy.

Some robot toys may only be controllable through an app. Other robots are fully interactive without the use of an app or controlling device. Anki's Cozmo, for example, has built-in spatial awareness and can move and interact independently with objects in the vicinity, including being able to detect faces and recognize the difference between cats and dogs. Still others, such as the Sphero BB-8, have limited independent features in addition to being controllable by an app. An accompanying app may provide ways to control the robot or change its characteristics, either through direct commands or through changes to the default settings.

Data collection from robotic toys can be extensive, as a robot typically needs to analyze a wide range of information from its surroundings in order to function. This may include geolocation information and spatial proximity, video and audio, infrared, and other forms of sensory data about the environment in which the robot is operating. In addition, customizable preferences themselves may have privacy implications to the extent that they reveal information about the user.[10] Robots may communicate with an accompanying app using short-range communication methods such as Bluetooth. These apps then typically connect to the Internet in order to utilize cloud-based infrastructure or externals servers. *See* Appendix I.

In evaluating the privacy implications of robotic toys, parents and consumers should consider what types of data are collected, and whether data is processed locally or externally. As robots become more advanced, they may necessarily collect more information. However, they may also become more capable of processing data locally, or operating effectively with more limited forms of data.

Wearables are connected toys that are primarily worn as accessories, such as bracelets, armbands, or helmets that are equipped with sensors. Increasingly popular with children, wearables may collect a range of sensory and bodily data—e.g. precise location, acceleration, motion, heart rate, and activity levels.

Fig. 6. EMPIRE EVS (Recon Instruments and Empire Paintball) is an example of a connected wearable toy.

The Moff Band tracks a child's arm movements in order to react with different sounds for different gestures. Similarly, the Empire EVS, a connected paintball helmet, provides an on-screen map and uses GPS to allow players to visualize their location and the location of other players. Certain types of data collected by wearables, e.g. precise location or health data, is typically considered more sensitive and subject to stronger controls.[11]

Learning Development toys have the purpose of teaching children a skill, subject, or knowledge area. These toys are often designed to enable children to develop cognitive and behavioral skills outside the classroom. Grush, the smart toothbrush, connects to an app where children can play games while learning how to brush their teeth effectively. Osmo uses an app on a camera-enabled device in order to detect tangrams, or puzzle pieces, that children shape with physical objects on a table. Wiggy, an Internet-connected piggy bank, is designed to help children learn basic financial skills.

Fig. 7. Osmo (Tangible Play) is an example of a connected learning development toy.

Learning development toys do not necessarily differ from other toys in the amount or quality of data collected, although they will often collect in-depth information with respect to a particular skill. For example, Grush will have detailed information on children's usage of their connected toothbrush.

New and Non-Traditional Uses for connected toys are rapidly emerging. Connected toys are appearing outside of the home, in settings such as hospitals and classrooms. They may also be used for specialized or new purposes, such as enabling children to send messages to family members.

In healthcare, connected toys may be used to enable pediatric care for patients who are undergoing intensive procedures, including to help manage anxiety and boost confidence, and to allow parents to monitor their children's health.[12] For example, the Huggable, an interactive teddy bear designed by the MIT Media Lab, is used in hospitals to interact with cancer patients and collect data in order to make their hospital visits more comfortable.[13] Connected toys are also being used as therapeutic devices for children with disabilities. For example, Beamz, a musical device, uses eye gaze detection and other technology to provide a wide range of therapeutic services for cognitive, physical, and social or emotional development.[14]

Fig. 8. Dino (CogniToys) is an example of a connected toy that may be used in classrooms.

In classrooms, connected toys such as Dino may be used to engage children in educational games and activities.[15] Some companies are bringing toys into new territories including financial services, such as Spiral Toys Inc., which is developing a credit card to go along with its Wiggy toy, a connected piggy bank, that will allow parents to provide financial and bank account information to the app in order to give their children allowances or pay for chores.[16]

While data collected by these toys may vary greatly, data that is otherwise subject to sector-specific privacy legislation may not be exempted if collected via a toy interface. For example, the Health Information Portability and Accountability Act (HIPAA) will apply to medical records even if such data is collected from a child patient via a toy.[17] Additionally, in a classroom setting, depending on the toy's functions, student data laws such as the Family Educational Rights and Privacy Act (FERPA) may apply.[18] Furthermore, the application of these kinds of sectoral laws will not necessarily fulfill the independent requirements of COPPA. Other contexts may simply mean that greater transparency or notice and control mechanisms may be appropriate.

II. The Legal Limits: COPPA is the Primary Privacy Law Regulating Data from Connected Toys

Although the Children's Online Privacy Protection Act (COPPA)[19] was written long before a mainstream market for connected toys existed, there is a growing consensus[20] that the federal statute applies to the wide range of modern toys that connect to the Internet. Most connected toys available today connect to the Internet through a mobile app or other mechanism, *see* Part I, and it is well-established that COPPA applies to Internet-connected devices and platforms, including smartphones, tablets, and apps.[21] The Federal Trade Commission (FTC) is vested with the legal authority to interpret COPPA, and it has promulgated more detailed requirements in the COPPA Rule.

COPPA applies to any provider ("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 . . .".[22] Although the FTC has not yet taken an enforcement action against a connected toy operator, the Commission has stated that the term "online service" broadly covers any service available over the Internet or that connects to the Internet or a wide-area network. This includes mobile apps, as well as network-connected games, Internet-enabled gaming platforms, social networking activities, and Internet-enabled location-based services.[23] Importantly, COPPA does not apply if an adult provides information *about* a child under 13, so long as the service is not also collecting personal information directly *from* the child.[24]

COPPA Applies to the Collection, Use, and Sharing of "Personal Information"

COPPA's definition of "personal information" is quite broad, and includes: names; addresses; online contact information; screen or user names; telephone numbers; Social Security numbers; photographs, video, or audio containing the child's image or voice; geo-location; and persistent identifiers that can be used to recognize a user over time and across different Web sites or online services (e.g. cookies or Device IDs).[25] This broad definition may even include types of information not usually considered personal information.[26]

Fig. 9. Furby Connect (Hasbro) is a connected toy that can be used and played without having to sync to an accompanying app.

Thus, some smart toys may not be required to seek parental permission if they collect or transmit only non-personal data. Non-personal data might include, for example, a child's keypress responses, the achievement level reached in a game, or whether a doll is giggling or talking.

Connected toys may similarly not be required to seek parental consent if they collect and use a persistent identifier, such as an IP address or Device ID, as long as the persistent identifier is used solely to support the internal operations of the service. Internal operations can include personalizing content at the user's direction (such as saving a game score), maintaining and analyzing the service, and performing network communications. An exception to COPPA-mandated parental consent requirements exists for these limited purposes.[27]

For example, the Furby Connect, a plush toy that speaks and responds in limited ways to external cues, such as being tickled or turned upside down, can be given to a child "out of the box." It can also sync via Bluetooth with an accompanying app (Furby Connect World). This sort of toy may not be required to seek parental consent even if it collects a persistent identifier, so long as they are used for the purposes described above.[28]

Other connected toys are designed to work out of the box, but may include additional, optional features that later require consent. For example, Disney's Playmation explains that Marvel's Avengers (action figures that sync with wearable

Avenger Gear) capture only *"gameplay activity data . . . including: leveling up, rewards, and abilities acquired."*[29] This "non-personal" gameplay information is paired with personal information only if and when the Gear is registered with the AvengersNet app and synced with a user account, which incorporates parental consent and access.

Many Connected Toys Provide or Include "Online Services" and Connect via the Internet

As described in Part I and Appendix I, the majority of connected or smart toys available today can reasonably be considered to incorporate online services, as they are typically (1) linked to a mobile application; and/or (2) connected to the Internet via Wi-Fi, 3G, 4G or LTE. This is the case regardless of whether the connected toy *itself* has a screen, as most connected toys rely on a mobile app or website for their initial set-up, and afterwards connect to the Internet in order to perform their basic functions.

The scope of COPPA is defined as applying to practices "in connection with the collection, use, and/or disclosure of personal information from and about children ***on the Internet***."[30] COPPA defines "Internet" broadly: "the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission."[31]

As written, therefore, COPPA only applies to services that collect information via TCP/IP protocols or successor protocols to TCP/IP. This would include, for example:

- Wired Internet connections
- Wi-Fi
- 3G, 4G, and other wireless services typically provided by telecommunications carriers

By definition, then, COPPA may not apply to toys that employ non-Internet forms of communication for limited purposes. Examples might include toys that communicate *only* with each other via Bluetooth, or other short-range protocols that do not typically rely on TCP/IP, e.g. Zigbee, Z-Wave, or others, at least to the extent the information is not thereafter transmitted to a server via TCP/IP. We have not identified any widely available toy that is capable of transmitting data to a remote server via a non-Internet protocol.

Also excluded are certain smart toys, described in Part I, that provide electronic interaction with children but operate locally and do not "collect" information "on the Internet." For example, the battery-operated Talk-to-Me Mikey operates locally to provide different responses based on different spoken questions, but does not connect to the Internet or transmit data externally. However, as soon as personal information is transmitted via Internet protocols, even if collected via a screen-less children's toy, COPPA requirements almost certainly attach. *See* Appendix I.

Many Connected Toys Are "Directed to" Children or Mixed Audiences

The FTC will likely consider many of the connected toys discussed in this paper to meet the COPPA test of being "directed to" children under 13. In determining whether an online service is targeted to children, the FTC considers the totality of the circumstances, including "subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content . . ."[32] As a result, many of the technologies marketed as toys today will be considered "directed to" children.

Whether a service is directed to children, in whole or in part, is a fact-specific inquiry. For instance, it is not enough for a company to state in a privacy policy that its service is only directed to individuals 13 and older. The FTC employs the fact-based test above to determine whether the service is "directed to" children, based on all available factors.

More challenging cases arise when toys are directed towards teenaged children, such as certain robotics or gaming systems. The CHiP

Robot Toy Dog by WowWee, for example, is recommended for ages 6-15 years,[33] and may appeal to broad audiences. However, the FTC has long recognized that online services directed towards older individuals may appeal to children under 13 as well. The FTC has carved out a narrow distinction for a service which may appeal to children under 13 but does not target children under 13 as its "primary audience."[34] These so-called "mixed-audience" sites are still subject to COPPA, but are permitted to employ an age screen to identify which of their users are under 13 so that they may get parental consent to collect information only from those users.[35]

Finally, an online service operator may fall under the reach of COPPA even if they are not targeting children, but instead have "actual knowledge" of personal information collected from children. This possibility is discussed further below, in the context of general home devices.

COPPA Offers Strong Legal Protections for Children's Data

For the operators of online services within its scope, COPPA requires a variety of mechanisms designed to provide parents with control over their children's information. These requirements include: providing notice; obtaining verifiable parental consent; mechanisms for parental review and revocation of consent; not conditioning a child's participation in a game or other activity on the child disclosing more information than is reasonably necessary to participate; and maintaining reasonable procedures for protection of confidentiality, security, and integrity of the information collected from children.[36] Importantly, though COPPA provides for limited exemptions,[37] this stringent legal regime applies strict liability and provides for statutory penalties of $40,000 per violation.[38]

Notice of Data Practices. COPPA requires operators to provide direct notice to parents of the operator's data collection practices. Direct notice must include certain statements, including how consent can be given, and that the operator will not collect, use, or disclose any personal information from the child until consent is given. The operator must state the items of personal information the operator intends to collect or disclose, and must also provide a link to the operator's privacy policy.[39] As the FTC clarified in 2013, key information must be presented to parents in a succinct "just-in-time" format.[40]

Verifiable Parental Consent. Before personal information can be collected from a child, the operator of an online service must obtain verifiable parental consent. The method of obtaining consent must take into account available technology to ensure that the person providing consent is the child's parent. COPPA lists several acceptable mechanisms, as examples, for obtaining consent, including:[41]

- Asking parents to sign and mail a physical consent form;
- Allowing parents to use a credit card or other online payment system that provides notification of each discrete transaction to the primary account holder;
- Having the parent express consent via phone or video conference; or
- Checking government-issued identification.

In the case where a company does not disclose children's personal information, an email paired with additional verification steps is sufficient.[42] As technology develops, the FTC encourages proposals for new methods of obtaining verifiable consent through its safe harbor approval process.[43]

Prohibition of Conditional Participation. Operators are prohibited from conditioning a child's participation in a game, offering of a prize, or other activity on the child disclosing more personal information than is "reasonably necessary" to participate.[44]

Reasonable Security. Operators are required to establish and maintain reasonable security procedures to safeguard the personal information collected from children.[45] The FTC elaborates reasonable security measures to mean minimizing data collection and only releasing data to third parties that can demonstrate and give assurance that their security measures comply with COPPA.[46]

Data Retention. COPPA requires that operators only retain personal information collected online from a child for as long as reasonably necessary to fulfill the purpose for which the information was collected. When the data is no longer needed to fulfill the purpose of collection, the data *must* be deleted using reasonable measures.[47] Parents also have the legal right to review and refuse further use or maintenance of personal information collected from a child.[48]

Enforcement Mechanisms

- *Penalties.* As of August 1, 2016, the maximum civil penalty for violating COPPA more than doubled from $16,000 to $40,000 per violation. One violation is counted for each child from whom an operator collects personal information in violation of COPPA. Thus, a connected toy directed at children under 13 with 1000 child users would face a potential civil penalty of up to $40,000,000.[49]
- *Voluntary Safe Harbors.* COPPA also provides voluntary Safe Harbors. By following the steps of a pre-approved Safe Harbor program, companies may be considered to be in compliance with COPPA.[50] As of October 2016, only seven Safe Harbor organizations have been approved.
- *Strict Liability.* Service operators who fall under COPPA are subject to "strict liability," which means that they may be held accountable for legal violations even if the violation was unintended. This accomplishes the FTC's goal of minimizing the burdens on parents by shifting responsibility to the child-directed content operators to ensure their compliance.[51]

COPPA May Apply Both to Toy Makers and Technology Providers

In the world of connected toys, the manufacturer of a teddy bear might be a different entity than the provider of the technology—the hardware and software—that connects the bear to the Internet. In these cases, COPPA could potentially apply to both companies.

A company that offers an online service covered by COPPA is responsible for all of the data collection that occurs on or through its service. In 2013, the FTC clarified that COPPA covers operators that design or control child-directed content, even if the children's data is collected by a third-party plug-in or ad network.[52] For example, a child-directed website that does not directly collect personal information from children would nonetheless be responsible for the data collection of third-parties that it permits to operate via its site.

Similarly, in the context of connected toys, a provider of a physical toy may be liable under COPPA even if that company does not itself collect personal information from children, but allows third parties to do so through a separate service that utilizes the toy as its interface. The toy provider will need to assess whether it must provide COPPA disclosures and obtain parental consent for the third-party's data collection practices, or whether it may rely on the third-party to do so. This determination may rest on the extent to which the third-party has a direct interaction with the child user. For example, if the child or parent is able to download a third-party app to the toy or affirmatively seek to access a third-party site or service through the toy, the third-party may be responsible for providing COPPA notice and consent mechanisms, although the first-party toy provider may need to directly notify parents that the toy permits access to third-party services which are governed by their own privacy policies and terms.

Under COPPA, the inquiry is highly fact-specific. It will be important for the toy provider to carefully monitor the data collection practices of any third-party it permits to operate through its toy. Additionally, the toy provider should address COPPA obligations contractually with any third-party it permits to operate through its toy.

COPPA may also apply to the upstream third-party operating through the toy. The FTC has stated that COPPA applies to a third-party, such as a plugin or ad network, when it has "**actual knowledge**" that it is collecting PII through a child-directed online service.[53] In the context of connected toys, it may be important for software

providers to understand the nature of the service through which its downstream customers may deploy the software. That upstream third-party could be independently liable for COPPA violations if it has actual knowledge that it is collecting information on or through a child-directed online service, including a toy.

Uncertainty may exist where a child-directed connected toy *platform*, such as EVS Empire, or Brixo Blocks (in development),[54] allows third-party applications to connect to the toy. In other contexts, general audience platforms such as the Apple App Store are not considered to be covered by COPPA, but a platform that is directed towards children may be treated differently.

General Home Devices Are Not Typically "Directed to Children" Within the Meaning of COPPA

The market for connected smart home devices is growing rapidly, but most general purpose home devices are not – and should not be – covered by COPPA. The federal children's privacy law applies only to online services that either directly target children or have actual knowledge that children are providing data through the device.

For good reasons, COPPA was not designed to apply to general audience online services, such as search engines or news websites, even though many children may indeed visit these websites and even provide personal information through them. As designed, COPPA requirements—for example, enhanced parental consent—are usually considered too burdensome to be applied to all the users of general audience services. Instead, these restrictions are considered appropriate for those operators who target children or have actual knowledge that they are collecting data from children. In part, this is because COPPA places heightened restrictions on the *user*, requiring users to undergo extra steps to provide verifiable consent before being able to access the service. In other words, it does not make sense for either operators or all users of a general market device to be burdened with the extra requirements of COPPA because of the possibility that a child might use that device.

In contrast, if a general purpose home device is directed to children, the device will fall under the umbrella of COPPA requirements. For example, the Smarty by Siliconic Home, Inc. (currently in development) is a child-facing home assistant designed to control lights, answer questions through a voice interface, and help with homework. This kind of device, described by the company's co-founder as an "Amazon Echo for kids," would most likely be considered "directed to" children under COPPA.[55]

Another way for a general audience website or service to fall under COPPA is for it to obtain **actual knowledge** that it is collecting data from children. This could include, for example, asking for a date of birth on the site's registration page, or asking "age identifying" questions like "What grade are you in?".[56] Most connected home devices do not obtain this knowledge, and would have to take extra privacy-intrusive measures to distinguish children from adults.

For example, a general audience device that utilizes speech recognition to interact with users may, at times, interact with children. However, these devices are typically engaged in speech recognition (speech to text) but not voice recognition (biometric identification).[57] As a result, they are unable to reliably distinguish age by voice with any accuracy in order to treat data from children differently than data from adults. With advancements in voice recognition technology, it may one day soon become possible to make such distinctions, and treat the data from children differently.

III: Privacy and Security: Strong Safeguards for Children's Data Can Help Parents Make Informed Choices

In light of the increasing popularity of connected toys, it is important for toy manufacturers and app operators to maintain strong privacy policies and responsible data practices when developing, selling, and updating connected toys and associated services.

Currently, 66% of parents report that they research, read reviews, and ask other parents for their connected toy recommendations.[58] 88% of these parents rely on product reviews, 71% look to blogs for recommendations, and 60% ask other parents for recommendations.[59] These figures demonstrate that parents are willing to spend considerable time gathering information from a variety of sources before buying products for their children. Additionally, children's own awareness and preferences affect the market, with 53% of parents reporting that the reason for purchasing a connected toy is because their child asks for it.[60] These figures highlight the key importance of developing appropriate privacy and security controls in order to enable parents to make informed decisions on the toys they purchase.

As discussed at the Kids & The Connected Homes event hosted by FOSI and FPF in 2016, toy providers should focus on certain key areas going forward, including improving notice and resources for parents, meaningful choice for parents, data minimization, and security by design.

In this Part, we explore three growing areas where privacy and security safeguards can help parents make informed choices, and help connected toy providers build trust: **Notice, Meaningful Choice, and Data Security.**

These recommendations, which go beyond a formulaic application of the Fair Information Practice Principles (FIPPs), can help ensure that data practices are fair and provide adequate protection for parents and children. At heart, toy makers should focus on smart design, and approach practical privacy issues with attitudes of trust and stewardship towards children.

Privacy and Security Implications of Non-Connected Toys Are More Limited

Smart toys have many benefits, helping children expand vocabulary or learning other skills. Many smart toys on the market today are designed to be adaptable and to collect limited forms of data in order to interact with children. When toys provide interactive features but do not connect to the Internet, privacy and security concerns are more limited.

Although non-connected toys do not typically pose concerns regarding remote data collection and use, toy manufacturers and technology providers should nonetheless be aware of parental concerns regarding the sociological or educational implications of smart toys.[61] Even when a toy does not transmit data, children may be exposed to marketing or may use a toy in a way that is harmful to their emotional or cognitive development. Research regarding the positive and negative impacts of smart toys will continue; we may yet be only beginning to understand the effects of smart toys, especially robot toys, on children's development.

Non-connected toys may raise privacy concerns to the extent that they may broadcast hardware-specific information that allows for detection or tracking from nearby sensors. For example, many non-connected toys may use Bluetooth BLE to allow different parts of the toy to interact with a physical controller or with different Bluetooth-enabled objects. If the toy is taken into a retail establishment or an airport that uses location analytics services, the hardware identifiers from the toy can be logged by those services. Toy manufacturers should be aware of this possibility and consider technical or policy measures to ensure that the toy can be used in public spaces while providing parents with appropriate privacy options.[62]

Notice: Toys Makers and Technology Providers Should Ensure That Parents Understand Data Practices

Providers of connected toys use data to enable the toy's functionality, and to develop and improve products over time. However, toy makers and technology providers also have an important incentive to ensure that parents who purchase connected toys for their children feel comfortable with the data being collected and how it is used.

Connected toys present unique challenges for notice: they are intended to be portable and screen-less, and often designed to integrate their sensors or hardware such that a casual observer might not distinguish between a connected and non-connected toy. Furthermore, although they may incorporate online services, connected toys are often, if not primarily, purchased in brick-and-mortar stores.

Providers of connected toys can build trust in their products by going beyond COPPA and focusing on awareness in all stages of product design and development, including with consistency across platforms, package labeling, and flexible and creative forms of notice.

Clear privacy notices Should Be Accessible Across Platforms. Companies should aim to be as open and public about their data practices as possible. A good first step is to provide clear and concise "just in time" privacy notices at points where the service is most likely to be interacting with parents when he or she is setting up the toy, such as during the initial download of an app, or during account registration. Companies can augment these notices with clear and prominent notices in other places where the parent might interact with the toy, such as the product manual, the associated app, and the product and/or company website.

In addition, shopping for connected toys often happens in retail stores, where COPPA does not require a privacy disclosure. Parents should be able to **understand at the point of sale**—before bringing it home to their child—whether or not they will later be asked to consent to the toy's collection of their child's personal information.

A full privacy policy on the box is not likely to be helpful, but some sort of cue will help parents decide before purchasing whether they are comfortable with the toy or whether they would like to do more research. For example, a toy's packaging could say: "Parents, this toy will require that you create a personal online account in order to access all features" or "Parents, this toy will require your permission to use your child's information to bring the toy to life!". This is in line with other well-recognized disclosures on packaging ("Batteries not included" or "sold separately"). See, e.g., Figure 10.

Fig. 10. Packaging label notice on Fischer-Price's connected toy, Smart Toy.

For example, many companies, if they have a privacy policy, may only post it on their website, where parents who interact only with the app might not know to look for it. Notice should be present and accessible in places where a parent can reasonably be expected to interact with the service, including at the point of app installation and within any associated apps.

Flexible and Creative Forms of Notice Will Help Build Intuitive Understanding. In the world of connected toys, many of which are screen-less, it is particularly important to consider notice holistically. Companies should invest in developing creative and intuitive ways to alert children and parents when data is being collected or transmitted—including glyphs, and other visual, audio, and haptic cues. The Hello Barbie Dreamhouse, for example, has a visible Wi-Fi indicator at the top, and responds to a spoken "wake phrase" by lighting up and making a beeping sound.

The form of notice may be related to the unique design of the toy and the way it interfaces with children. For example, if a connected toy is

primarily voice-enabled, it can provide a basic form of notice upon hearing voice commands related to privacy, as is now done by the Hello Barbie. If a connected toy is primarily controlled through an app, it will be important to make the privacy notice prominent and easily readable within the app.

These kinds of notices, which will remain flexible and adapt over time, will help ensure that the physical toy itself is intuitive, and will not surprise parents with unexpected data collection.

Flexible and creative forms of notice will also help providers address the question on many parents' minds: what if my child's friend brings over a connected toy? Although, as we explain in Part II, obtaining consent from other parents is most likely not desirable or feasible (given the privacy-intrusive methods that would be needed to distinguish between children), toy providers may nonetheless be well-served to consider how outside observers may react to a connected toy. From this perspective, there is an increasing utility for built-in visual, audio, or haptic cues.

Companies should also be conscious of the wide range of users, including children or parents with disabilities who may benefit from adaptable forms of notice and controls. Implementing user education and clear settings is one step in ensuring that users are fully aware of when data is flowing between a physical toy and a computer server.

Choice: Parents Should Be Able to Consent in Meaningful Ways to Data Collection and Use

Federal law, as explored above, requires that a provider obtain verifiable parental consent for the collection, use, or disclosure of any personal information collected from children (with narrow exceptions, see Part II).

However, beyond adhering only to COPPA's requirements, toy providers would be well-served to invest in thought and smart design to make parents feel comfortable with their options for data collection and use. Options should be customizable, granular enough to provide meaningful choices without being overwhelming, and easily understandable.

A good first step for obtaining meaningful consent is to alert parents at the point of sale that their consent will be needed (discussed above). After a parent has purchased a toy, especially if there is a child who is asking for the toy, they are much less likely to withhold their consent to its data practices.

Currently, all connected toys reviewed in this paper have an associated app or online interface in which parents can give consent to data collection. Thus, the design of the associated mobile apps will be critical. Although mobile operating systems may not currently require it, providers of connected toys should post prominent privacy notices in the App Stores, as well as within the app itself and any other platform that the parent might be expected to access.

Consent mechanisms within the app or online account should be **usable**. In order for parents to meaningfully have control over the sharing and uses of their child's information, companies should put serious thought into the user interface and granularity of consent options. It is important to ensure that they are intuitive enough that parents have control, but not so complex that they risk being overwhelming.

Increasingly, operating systems are requiring more granular and nuanced controls. Apple's iOS 10, for example, requires that apps request permission for sensitive categories of data within the app itself ("just-in-time" consent), rather than permitting the user to provide blanket consent to all app permissions upon download.

Security: Safeguarding Data Helps Mitigate Risks of Unauthorized Disclosure

Providers of connected toys, especially those that collect personal information, have a responsibility to safeguard that information. Leading toy companies recognize the need to implement strong security measures, especially as the FTC can bring enforcement actions against companies with inadequate security practices (with heavy monetary penalties, *see* Part II above).

Other toy companies may not be as aware of leading practices, or as expert in determining what security measures are appropriate. With varying levels of sophistication, it is increasingly important to collaborate amongst industry to identify and share leading practices.

Here, we identify a number of key considerations for security design, given concerns such as remote access to sensors and other data, intruders being able to turn devices on or off or otherwise manipulate the device's behavior, and other routes to unauthorized disclosures.

While these considerations will not alone guarantee that an app or platform has incorporated all necessary security measures, they provide a starting point for integrating strong cybersecurity into toys.

Companies can take a variety of important steps to safeguard their data:

- Identify vulnerabilities by conducting independent security audits;
- Facilitate ongoing identification of vulnerabilities by communicating with the security community and being involved in a public Bug Bounty Program;[63]
- Determine when local processing, remote processing, and third-party sharing is appropriate, and mitigate security risks for the selected approach to data processing;
- Implement strong encryption standards (HTTPS / TLS) so that the toy will not send personal information over insecure channels, or store personal information in an insecure format on the toy itself;
- Ensure that strong encryption standards prevent the toy from communicating with unauthorized devices or servers;
- Do not use passwords that cannot be changed by users, and do not use the same default password for all toys;
- Ensure that access to any remote server is secure by using physical and administrative restrictions, as well as technical restrictions (such as preventing unauthenticated firmware updates) or implementing IP address whitelisting;
- Be aware of emerging industry norms regarding: (1) how to ensure that connected devices can receive security updates, and how companies can communicate update capabilities to consumers;[64] (2) how to best disclose and respond to disclosures regarding security vulnerabilities;[65] and (3) how to work with peer companies and the public sector to share information related to cybersecurity risks and coordinate responses.[66]

Connected devices have suffered security breaches in a range of contexts in recent years.[67] Home security cameras have been compromised, allowing unauthorized parties to view video from the inside of unsuspecting consumers' homes.[68] Many reports have surfaced of unauthorized people accessing baby monitors and speaking, sometimes offensively, to children.[69] Similar sensors (including video cameras and microphones) are used in some connected toys as are used in these general home devices. If similar vulnerabilities are exposed in toys, the security breach would potentially allow bad actors to access video of children, audio of children, or use the toy to communicate with children. Thus, in the context of connected toys, the sensitivity of the audience makes concerns over security even more critical. [70]

As the number of connected toys continues to grow, cybersecurity will become an increasingly prominent issue.[71] Currently, 90% of connected devices are collecting personal information and 70% are transferring that information over unencrypted networks.[72] If companies focus on security by design, connected toys can go onto the market already vetted to protect data, giving consumers a reputable source of entertainment for their children.

CONCLUSION

Advances in technology are creating new possibilities for parents and children that once could hardly have been imagined. Children are now able to converse with dolls, play digital games with physical teddy bears, battle each other with robots from different parts of the world, and engage in creative storytelling through wearable virtual gear. Connected toys are also being used in pediatric healthcare for treatment and diagnosis, and are breaking into other new settings such as education and therapy. Some toys are also enhancing accessibility, helping children with disabilities experience new areas of play never possible before. In order to provide these cutting-edge features, many toys connect to the Internet to harness the power of cloud-based computing.

Connectivity, though, raises concerns over privacy and security of data collected from children. Legal restrictions provide baseline safeguards for children's privacy. The federal Children's Online Privacy Protection Act (COPPA) proves to be versatile, adaptable, and applicable to new technologies. Beyond adhering to rules and regulations, companies should go beyond COPPA's strictures by building privacy into the design and packaging of their toys. Privacy by design will truly build trust and confidence in connected toys. Equally important, good privacy practices include strong security measures, and concerns regarding cybersecurity threats in the general Internet of Things sector apply even more strongly to connected toys.

The future for connected toys is promising, but more can be done to build trust with parents and children. Industry leaders that follow privacy and security best practices, including those described here, will be well suited to succeed in the growing market for connected toys.

END NOTES

[1] Future of Privacy Forum & Family Online Safety Institute, *July 20th Event: Kids & The Connected Home*, (Jul. 20, 2016), https://fpf.org/2016/07/06/kids-connected-home/ (video of the event is available at https://www.youtube.com/watch?v=wk_gr1a0QjA).

[2] *See* JUNIPER RESEARCH, *Smart Toys: Do Toys Dream of Digital Lives?* (Nov. 2015), *available at* https://www.juniperresearch.com/document-library/white-papers/smart-toys-~-do-toys-dream-of-digital-lives (reporting that the smart toy market was projected to hit $2.8 billion by 2015 and $11.3 billion by 2020, in comparison to a total of toy industry sales of $22 billion in 2015). *See also* Andy Robertson, *Connected Toys Are Only Just Getting Started, Here's What's Next*, FORBES (Apr. 21, 2016), http://www.forbes.com/sites/andyrobertson/2016/04/21/connected-toys-venture-capital-report/ (discussing how venture capitalist funding of connected toys has steadily and rapidly increased since 2012); Doug Renert, *The Serious Business Of* Play, TECHCRUNCH (Feb. 15, 2016), https://techcrunch.com/2016/02/15/the-serious-business-of-play/.

[3] *See* Lauren Orsini, *How Tamagotchi Rose From The Dead To Join The Internet Of Things*, FORBES (Jul. 1, 2015), http://www.forbes.com/sites/laurenorsini/2015/07/01/how-tamagotchi-rose-from-the-dead-to-join-the-internet-of-things/#99af12d533c8.

[4] *See* Sony, *Aibos History*, http://www.sony-aibo.com/aibos-history/ (last accessed Nov. 23, 2016).

[5] Advances in speech recognition allow for the ability to speak naturally and contextually with a computer system in order to translate speech to text or execute commands. Voice recognition, in contrast, involves biometric identification of an individual by the characteristics of her voice. Many general home devices on the market today use speech recognition as their primary interface. *See* STACEY GRAY, FUTURE OF PRIVACY FORUM, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES (Apr. 2016), *available at* https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

[6] An example of a very smart connected toy is CogniToys' Dino, an interactive talking dinosaur developed by Elemental Path. Dino is able to discuss topics with children in detail and learn their preferences over time, and provides a greater level of interaction by connecting via Wi-Fi to IBM's Watson, a cloud-based artificial intelligence service. *See* CogniToys, *How It Works*, https://cognitoys.com/pages/about (last accessed Nov. 23, 2016).

[7] *See* note 60.

[8] *See, e.g.*, Brendan Sinclair, *Toys-to-life grew 7% in 2015 – NPD*, GAMESINDUSTRY.BIZ (Apr. 21, 2016), http://www.gamesindustry.biz/articles/2016-04-21-toys-to-life-grew-7-percent-in-2015-will-shrink-in-2016-npd; David Roberts, *What is the 'toys-to-life' genre, anyway?*, GAMESRADAR (Nov. 23, 2015), http://www.gamesradar.com/what-is-toys-life-genre-anyway/.

[9] *See* Doug Renert, *The Serious Business Of* Play, TECHCRUNCH (Feb. 15, 2016), https://techcrunch.com/2016/02/15/the-serious-business-of-play/ (citing research by Tandem Capital that in 2015, the total amount of venture capitalist funding given to connected toy start-up companies placed 64% of the total amount invested in robotics, 29% in learning development, 5% in toys to life, 3% in other).

[10] In addition to collecting data from sensors, a robot may have customizable preferences that reveal information about its user. *See generally,* Ryan Calo, *Robots and Privacy*, in *Robot Ethics: The Ethical and Social Implications of Robotics*, Patrick Lin, George Bekey, and Keith Abney, eds. (Apr. 2, 2010), pg. 3, 13-14, *available at* https://ssrn.com/abstract=1599189 (describing "settings privacy," including how the ways in which a person programs a robot might be intimately revealing).

[11] *See* FUTURE OF PRIVACY FORUM, BEST PRACTICES FOR CONSUMER WEARABLES & WELLNESS APPS & DEVICES (Aug. 17, 2016), https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf.

[12] Increasingly, toys are being used as a tool for medical professionals or to help parents monitor their children's health. For example, Grush, a connected tooth brush, allows parents to send collected data on their children's

brushing habits to dentists. *See* IBM, *Grush: From entrepreneur to reality TV star* (last accessed Nov. 27, 2016), https://developer.ibm.com/startups/grush/. Jerry the Bear, a connected teddy bear that teaches children with diabetes how to be healthy, may collect health information about a child from parents, such as date since diagnosis. Sproutel, *Jerry the Bear Privacy Policy*, https://www.jerrythebear.com/legal.html (last accessed Nov. 27, 2016). Research indicates that smart toys may also prove beneficial for early diagnoses of medical conditions. *See, e.g.*, Maria Luisa Martin-Ruiz, Miguel Angel Valero, Maria Linden, Susana Nunez-Nagy, Angeles Guiterez Garcia, *Foundations of a Smart Toy Development for the Early Detection of Motoric Impairments at Childhood*, INT'L J. OF PEDIATRIC RESEARCH (Nov. 11, 2015), *available at* http://clinmedjournals.org/articles/ijpr/international-journal-of-pediatric-research-ijpr-1-011.pdf (describing the development of a smart toy for the early detection of motoric impairments).

[13] *See* MIT Media Lab, *Personal Robotics Group, Huggable*, http://robotic.media.mit.edu/portfolio/huggable/ (last accessed Nov. 23, 2016); The New York Times, *A Talking Teddy Bear Practicing in the Pediatric Hospital*, THE NEW YORK TIMES (Jun. 3, 2015), http://www.nytimes.com/2015/06/04/technology/huggable-robot-therapeutic-value-hospitals.html?_r=0.

[14] *See* Beamz Interactive, *Beamz For Therapy & Rehab*, http://www.thebeamz.com/therapy-rehab/ (last accessed Nov. 23, 2016).

[15] *See* CogniToys *Meet the CogniToys Dino*, https://cognitoys.com/ (last accessed Nov. 23, 2016); Elemental Path, *The Educational Toy Dino Unlike Any Other | CogniToys* (Jan. 21, 2016), *video available at* https://vimeo.com/152622607.

[16] Spiral Toys is developing a credit card to accompany its connected toy piggy bank, Wiggy, which will allow parents to set-up a debit card for their children from their Wiggy account. *See* Spiral Toys, *Spiral Toys Provides Product Update and 2016 Outlook*, Spiral Toys Blog, News, Press Release (Jun. 30, 2016), http://spiraltoys.com/spiral-toys-provides-product-update-and-2016-outlook/.

[17] *See* Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (Aug. 21, 1996), *available at* https://www.gpo.gov/fdsys/pkg/STATUTE-110/pdf/STATUTE-110-Pg1936.pdf.

[18] *See* Family Educational Rights and Privacy (FERPA), 34 CFR § 99, 53 FR 11943 (Apr. 11, 1988), *available at* http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5.

[19] Children's Online Privacy Protection Act (COPPA), 15 USC §§ 6501-6508, 16 CFR § 312, 78 FR 4008 (Jan. 17, 2013), *available at* http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5.

[20] For example, former FTC Commissioner Julie Brill has expressed that she believes that the FTC would view COPPA as applying to connected toys. *See* Future of Privacy Forum & Family Online Safety Institute, *July 20th Event: Kids & The Connected Home*, (Jul. 20, 2016), https://fpf.org/2016/07/06/kids-connected-home/ (video of the event is available at https://www.youtube.com/watch?v=wk_gr1a0QjA).

[21] *See* Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions,* (Mar. 20, 2015), FAQ A.9, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[22] 16 CFR § 312.3. COPPA defines "operator" as any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation.

[23] *See* note 21.

[24] The age of 13 was chosen because Congress recognized that younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues presented by the online collection of information. *See* Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions,*

(Mar. 20, 2015), FAQ A.11, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[25] 16 CFR § 312.2.

[26] As an example of unusual data that may be considered "personal information," consider chess moves. Square Off, a connected chess board (in development), may collect game play data such as a user's favorite signature moves and habits. Square Off, *Square Off – World's Smartest Chess Board*, Kickstarter, https://www.kickstarter.com/projects/infivention/square-off-worlds-smartest-chess-board-relaunched (last accessed Nov. 27, 2016). Many chess players consider their style of play to be personal and possibly unique, to the point that some chess players have attempted to copyright certain moves or games. *See* Mark Borders, *The Self-Improvement of Chess* (2007), at 51; Murray Whyte, *Can you copyright a chess move?*, THE STAR (Mar. 15, 2009), https://www.thestar.com/news/insight/2009/03/15/can_you_copyright_a_chess_move.html; Edward Winter, *Copyright on Chess Games* (last updated Mar. 12, 2016), http://www.chesshistory.com/winter/extra/copyright.html.

[27] *See* 16 CFR § 312.5(c)(7); Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions,* (Mar. 20, 2015), FAQ I.5, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[28] *See* Hasbro, *Hasbro Mobile Application Privacy Policy* (last Updated Nov. 14, 2016), http://www.hasbro.com/app_esrb_privacy.

[29] The Walt Disney Company, *Playmation & Your Privacy* (last accessed Nov. 23, 2016), http://www.playmation.com/privacy.

[30] 16 CFR §312.1.

[31] 16 CFR 312.2.

[32] *See* Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions,* (Mar. 20, 2015), FAQ G.2, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[33] Amazon.com, *CHiP Robot Toy Dog – White*, WowWee, https://www.amazon.com/WowWee-CHiP-Robot-Toy-Dog/dp/B01CFW6ME8/.

[34] *See* Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions,* (Mar. 20, 2015), FAQ G, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[35] *See* note 34.

[36] 16 CFR § 312.

[37] COPPA lays out limited exemptions. For example, operators that collect a persistent identifier and no other personal information solely to provide internal operations do not need to provide notice. *See* 16 CFR § 312.5(c)(7).

[38] Federal Trade Commission, Adjustment of Civil Monetary Penalty Amounts, 81 Fed. Reg. 42476 (June 30, 2016) (to be codified 16 C.F.R. pt. 1), *available at* https://www.ftc.gov/system/files/documents/federal_register_notices/2016/06/160630civilpenaltyfrn.pdf.

[39] 16 CFR § 312.4(c)(1).

[40] Federal Trade Commission, 78 Fed. Reg. 12, 3984-85 (Jan. 17, 2013), *available at* https://www.ftc.gov/system/files/2012-31341.pdf.

[41] 16 CFR § 312.5(b)

[42] 16 CFR § 312.5(b)(2)(vi).

[43] 16 CFR 312.5(b)(3); *see also* note 40, pgs. 3991-2.

[44] 16 CFR § 312.7.

[45] 16 CFR § 312.8.

[46] *See* note 40, pgs. 3994-95; *see also* Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* (June 2013), Step 6, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step6.

[47] 16 CFR §312.10.

[48] 16 CFR § 312.6.

[49] *See* note 38.

[50] 16 CFR § 312.11

[51] *See* note 40, pg. 3975-77.

[52] *See* note 40, pgs. 3975-78.

[53] *See* note 40, pgs. 3975-78.

[54] Brixo Blocks, *Brixo - Building Blocks Meet Electricity and IoT*, Indiegogo, https://www.indiegogo.com/projects/brixo-building-blocks-meet-electricity-and-iot-diy#/ (last accessed Nov. 27, 2016).

[55] *See* Siliconic Home, *Smarty: An Intelligent Connected Device for Kids*, http://www.siliconichome.com/ (last accessed Nov. 27, 2016); Zoe Corbyn, *The future of smart toys and the battle for digital children*, THE GUARDIAN (Sept. 22, 2016), https://www.theguardian.com/technology/2016/sep/22/digital-children-smart-toys-technology.

[56] Federal Trade Commission, *When Does The Operator of a Website or Online Service Have "Actual Knowledge" of Someone's Age?*, Children's Online Privacy Protection Rule: Not Just for Kids' Sites (Apr. 2013), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites.

[57] *See* note 5.

[58] BSM Media, Digital Kids Media, *Parents, Kids Drive Billion-Dollar Smart Toy Market* (Feb. 15, 2016), http://www.bsmmedia.com/2016/02/parents-kids-drive-billion-dollar-smart-toy-market/.

[59] *See* note 57.

[60] *See* note 57.

[61] There have been concerns expressed in recent years by parents and other advocates that smart toys may impact children's cognitive development, creativity, or imagination. *See, e.g.,* Jason Bogg, *Hello Barbie's war on imagination: The childhood-destroying gift you don't want to give your kid*, SALON (Dec. 19, 2015), http://www.salon.com/2015/12/19/hello_barbies_war_on_imagination_the_childhood_destroying_gift_you_dont_want_to_give_your_kid/. Research indicates potential drawbacks as well as potential benefits to children. *See, e.g.*, Anna V. Sosa, *Association of the Type of Toy Used During Play With the Quantity and Quality of Parent-Infant Communication*, JAMA PEDIATRICS (Feb. 2016), *available at* http://jamanetwork.com/journals/jamapediatrics/article-abstract/2478386 (concluding that smart toys may impede language learning). *But see* Jeffrey Goldstein, *Play In Children's Development, Health and Well-being*, TOY INDUSTRIES OF EUROPE (Feb. 2012), *available at* http://www.ornes.nl/wp-content/uploads/2010/08/Play-in-children-s-development-health-and-well-being-feb-2012.pdf (concluding that smart toys can facilitate children's speech vocabulary, and pre-reading skills).

[62] Companies should consider the technical options that may be feasible for ensuring that the toy can be used in public spaces without broadcasting hardware-specific identifiers. Options may include enabling on/off settings for

Wi-Fi or Bluetooth, or providing their range of toy-assigned MAC addresses to the industry's location analytics central Opt Out program. *See* Future of Privacy Forum, *Mobile Location Analytics Opt Out*, https://smart-places.org/ (last accessed Nov. 25, 2016).

[63] *See e.g.*, HackerOne, *Public Bug Bounty Program* (last accessed Nov. 27, 2016), https://hackerone.com/ (demonstrating a program that allows hackers to find security leaks and aid in creating a security program).

[64] *See e.g.*, National Telecommunications & Information Administration, *Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching* (last accessed Nov. 27, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (demonstrating an example of a working group that deals with security update solutions).

[65] *See e.g.*, National Telecommunications & Information Administration, *Multistakeholder Process: Cybersecurity Vulnerabilities* (last accessed Nov. 27, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities (demonstrating an example of a working group that deals with security vulnerability disclosures).

[66] *See e.g.*, President Barack Obama, *Executive Order -- Promoting Private Sector Cybersecurity Information Sharing*, The White House Office of the Press Secretary (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (demonstrating a method of how organizations can enter into secure information sharing to promote cybersecurity and coordinated responses).

[67] *See, e.g.*, Bruce Schneier, *Hacking Consumer Devices*, Schneier on Security (Aug. 23, 2013), https://www.schneier.com/blog/archives/2013/08/hacking_consume.html.

[68] *See e.g.* Tracy Clemons, *Bedroom Webcam Was Hacked*, ABC13 EYEWITNESS NEWS (Aug. 10, 2016), http://abc13.com/news/mom-learns-daughters-bedroom-webcam-was-hacked/1465134/; Ms. Smith, *Peeping into 73,000 unsecured security cameras thanks to default passwords*, NETWORK WORLD (Nov. 6, 2014), http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html.

[69] *See e.g.* Chante Owens, *Stranger hacks family's baby monitor and talks to child at night*, The San Francisco Globe (Nov. 29, 2016), http://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/.

[70] Many policymakers, including Senator Mark Warner, have expressed concerns over COPPA's application to connected devices that may expose children's data including baby monitors, dolls, and stuffed animals. *See* Seena Gressin, *Is your baby monitor secure?*, Federal Trade Commission Blog (Jan. 19, 2016), https://www.consumer.ftc.gov/blog/your-baby-monitor-secure; Senator Mark Warner, Press Release, *Sen. Warner Calls on FTC to Protect Children's Data Security with Internet-Connected 'Smart Toys'* (Jul. 6, 2016), http://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=CA5E4D0F-512A-4140-A8AF-006B9F387809.

[71] *See* The Associated Press, *Connected toys especially vulnerable to hackers, security experts warn*, CBCNEWS (Feb. 3, 2016), http://www.cbc.ca/news/technology/connected-toy-security-1.3431633.

[72] *See* Packard Enterprise, *Internet of Things State of the Union: Internet of Things Research Study* (Sep. 2014), *available for download at* http://go.saas.hpe.com/fod/internet-of-things.

APPENDIX I

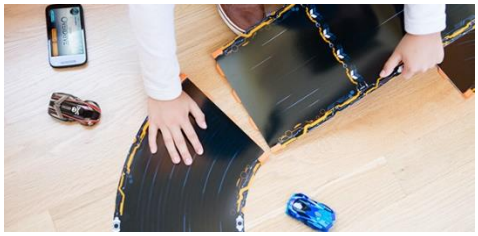
The following is an alphabetical list of noteworthy toys referenced in this white paper, most of which are smart or connected toys, or both. In Part I, we describe these categories and their privacy implications. For the connected toys listed below, we describe the toy's method of connection, user interface, and the permissions requested by its accompanying app.[1] We also identify where users can find a connected toy's privacy policy.[2]

1. Anki Overdrive by Anki, Inc.

Privacy Policy: https://anki.com/en-us/privacy

Description: Anki Overdrive is a set of physical race cars on a customizable race track. The cars pair via Bluetooth with an accompanying app which is used as a controller and as a way to customize the cars' features.

Categories: Connected.



Credit: Anki, Inc.

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**Photos/Media/Files** Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage **Wi-Fi connection information** Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices **Bluetooth connection information** Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices **Device ID & call information** Allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call

[1] For toys with an accompanying Android app, we enumerate the permissions listed in the Google Play App Store. The specific language is taken from the list of permissions prompted upon installation, or, if unavailable, from the description provided in the "Permission details" section of the app's landing page. This appendix does not include iOS request permissions because Apple recommends iOS developers to only request permissions when the "app clearly needs it," such as requesting a location permission only when a user activates a location feature within the app. Therefore, we would need to access each app and every single one of its functions before being able to conclusively state every permission each app requests. *See* Apple, "iOS Human Interface Guidelines: Requesting Permission" (last accessed Nov. 23, 2016), https://developer.apple.com/ios/human-interface-guidelines/interaction/requesting-permission/.

[2] We identify where users can locate a connected toys' privacy policy if it was available and easily accessible to us. If we do not list an accompanying privacy policy with a connected toy it may be because the toy is not legally required to have one, because the toy's company may have a privacy policy in a contract with a user such as in cases where a toy is explicitly used in special settings (e.g. in a hospital), or for other reasons.

2. BEAMZ by Beamz Interactive, Inc.

Description: Beamz is a music playing device that is designed to be physically accessible to everyone, including those with physical or mental disabilities. Accessibility includes eye gaze technology, allowing music to be played through eye movement detection. Used in schools, therapy and rehab sessions, and at home, it pairs with a smartphone via Bluetooth or a computer with installed software via cable.

Categories: Connected.

Credit: Beamz Interactive, Inc.

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS) • Computer Software	**In-app purchases** Allows the user to make purchases from within this app **Identity** Uses one or more of: accounts on the device, profile data **Photos/Media/Files** Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage **Bluetooth connection information** Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices.

3. CHIP by Wowee Group Limited

Description: CHIP is a robot pet dog that comes with a smart ball and a wrist band. It pairs with a smartphone, a wrist band, and a small ball via Bluetooth.

Categories: Connected; Smart.

Credit: Wowee Group Limited

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**Photos/Media/Files** Uses one or more of: files on the device, such as image, videos, or audio; the device's external storage **Bluetooth connection information** Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices

4. Cozmo by Anki, Inc.

Privacy Policy: https://anki.com/en-us/privacy

Description: Cozmo is a robot with a personality that a user can control or play games with. It pairs with a smartphone via Bluetooth.

Categories: Connected; Smart.

Credit: Anki, Inc.

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**Camera** Take pictures and videos **Storage** Modify or delete SD card contents. Read content on SD card **Other** Allow Wi-Fi Multicast reception, full network access, Google Play license check, prevent phone from sleeping, connect and disconnect from Wi-Fi, pair with Bluetooth devices, receive data from Internet, access Bluetooth settings, control vibration, view network connections, via Wi-Fi connections.

5. Dino by CogniToys

Privacy Policy: https://cognitoys.com/privacy

Description: Dino is a physical toy that can be interacts primarily through speech recognition. Powered by IBM's Watson, it can converse intelligently. Dino functions, in a limited capacity, without connecting to the Internet, but it can also pair with a smartphone via Bluetooth to connect to Wi-Fi. Once connected, the Dino no longer requires the use of a smartphone for playtime. It updates automatically as new content becomes available.

Categories: Connected; Smart.

Credit: CogniToys

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**Location** Uses the device's location **Wi-Fi connection information** Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices

6. Edwin the Duck by pi lab, LLC

Credit: pi lab, LLC

Privacy Policy: The privacy policy is accessible on the app through the settings button.

Description: Edwin is a physical rubber duck that has features controllable through multiple apps. Some apps also include games. It pairs with a smartphone via Bluetooth.

Categories: Connected.

Interface(s):	Permissions Requested (Android M):
• Multiple apps (Android and iOS)	**Location** Approximate location (network-based), precise locations (GPS and network-based) **Storage** Modify or delete SD card contents, read content on SD card **Other** Full network access, pair with Bluetooth devices, change your audio settings, access Bluetooth settings

7. Empire EVS by Recon Instruments, Inc. and Empire Paintball

Recon Instruments, Inc.

Description: Empire EVS is a goggled-helmet used for playing paintball with a special display that uses GPS to show the current location of the player and team members in real-time. It pairs with a smartphone via Bluetooth or can directly connect to Wi-Fi and GPS. It can also connect to other paintball equipment to measure data such as shot count, rate of fire, and battery level.

Categories: Connected.

Interface(s):	Permissions Requested (Android M):
• App (Android and iOS) • Heads-Up Display on helmet	**Identity** Uses one or more of: accounts on the device, profile data **Contacts** Uses contact information **Location** Uses the device's location **SMS** Uses one or more of: SMS, MMS. Charges may apply. **Phone** Uses one or more of: phone, call log. Charges may apply. **Photos/Media/Files** Uses one or more of: files on the device, such as images, videos, or audio: the device's external storage **Bluetooth connection information** Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices. **Device ID & call information** Allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected

8. Furby Connect by Hasbro, Inc.

Credit: Amazon

Privacy Policy: http://www.hasbro.com/app_esrb_privacy

Description: Furby Connect is a physical interactive doll functions with or without an app. Some compatible apps have games on them. It pairs with a smartphone via Bluetooth.

Categories: Connected; Smart.

Interface(s):	**Permissions Requested (Android M):**
• Multiple apps (Android and iOS)	**In-app purchases** Allows the user to make purchases from within this app **Identity** Uses one or more of: accounts on the device, profile data **Photos/Media/Files** Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage **Camera** Uses the device's camera(s) **Bluetooth connection information** Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices.

9. Galaxy ZEGA by Smartx Network Technology Co., Ltd.

Credit: Smartx Network technology Co., Ltd.

Description: Galaxy ZEGA are physical tanks that can roam on most surfaces or on separate track accessories. An accompanying app acts as a tank's controller and a way to customize tank statistics and virtual features and control opponents' tanks. These tanks pair with a smartphone via Bluetooth.

Categories: Connected; Smart.

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**In-app purchases** Allows the user to make purchases from within this app **Device & app history** Allows the app to view one or more of: information about activity on the device, which apps are running, browsing history and bookmarks **Identity** Uses one or more of: accounts on the device, profile data **Location** Uses the device's location **Photos/Media/Files** Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage **Wi-Fi connection information** Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices **Bluetooth connection information** Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices. **Device ID & call information** Allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call

10. Grush by Grush, Inc.

Description: Grush is a toothbrush that serves as a motion sensing game controller for games on an accompanying app. It pairs with a smartphone via Bluetooth.

Categories: Connected.

Credit: Grush, Inc.

Interface(s):	**Permissions Requested (Android M):**
• Multiple apps (Android and iOS)	**Location** Approximate location (network-based) **Other** Pair with Bluetooth devices, access Bluetooth settings

11. Hello Barbie Dream House by Mattel, Inc.

Privacy Policy: https://www.toytalk.com/hellobarbie/privacy/

Description: Hello Barbie Dream House is a physical doll house that is Wi-Fi voice activated and recognizes 100+ commands. It also contains 50+ sounds and songs. It also functions without connecting to the Internet by enabling activation of its lights, sounds, and motors through switches. It pairs with a smartphone via Bluetooth, but after set-up, it can connect to Wi-Fi without use of the app.

Categories: Connected; Smart.

Credit: Amazon

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**Photos/Media/Files** Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage **Microphone** Uses the device's microphone(s) **Wi-Fi connection information** Allows the app to view information about Wi-Fi networking, such as whether Wi-Fi is enabled and names of connected Wi-Fi devices

12. Huggable by MIT's Media Lab

Credit: Gizmodo

Description: Huggable is a stuffed bear robot. Currently, it is being used by hospital specialists to communicate with patients and collect data. All children who interact with the toy wear a bracelet, called a Q sensor, to measure physiological changes. It pairs with a computer used by hospital specialists. The Q sensor bracelet also pairs with a computer via Bluetooth.

Categories: Connected.

Interface(s): Website browser, stale panorama of the camera, wearables that can control the bear's movement, and remote controller

13. Imaginarium Metro Line Train Table by Toys "R" Us, Inc.

Credit: Toys "R" Us, Inc.

Description: Imaginarium Metro Line Train Table is a physical table with accessories that children can physically control and alter.

Categories: Non-connected.

14. Kidizoom Smartwatch DX by VTech Holdings Ltd

Credit: Amazon

Description: Kidizoom is a smart watch that has preinstalled games, activities, camera, recorder, touch screen, calculator, calendar, an alarm, and a motion sensor. It does not connect to the internet or to any devices, though it can connect to another device using a cable in order for the user to transfer media from the watch onto another device.

Categories: Non-connected; Smart.

15. Love2Learn Elmo by Playskool Inc.

Privacy Policy: http://www.hasbro.com/app_esrb_privacy

Description: Love2Learn Elmo is a plush toy that can interact with children. An accompanying app has games on it. It pairs with a smartphone via Bluetooth.

Categories: Connected; Smart.

Credit: Hasbro, Inc.

Interface(s):	Permissions Requested (Android M):
• App (Android and iOS)	**Camera** Take pictures and videos **Location** Approximate location (network-based) **Phone** Read phone status and identity **Storage** Modify or delete SD card contents. Read content on SD card **Other** Full network access, prevent phone from sleeping, pair with Bluetooth devices, access Bluetooth settings, view network connections, view Wi-Fi connections

16. Moff Band by Moff, Inc.

Privacy Policy:
https://support.moff.mobi/moff_privacy_policy_en.html

Description: The Moff Band is a wearable bracelet that allows kids to be physically active by detecting arm and general movements. It uses an accompanying app to set gameplay features. Third-party apps are also available. It pairs with a smartphone via Bluetooth.

Categories: Connected.

Credit: Moff, Inc.

Interface(s):	Permissions Requested (Android M):
• Multiple apps (Android and iOS)	**Photos/Media/Files** Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage **Bluetooth connection information** Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices.

17. Osmo by Tangible Play, Inc.

Privacy Policy: https://www.playosmo.com/en/privacy-policy/

Description: Osmo is a set of physical accessory toys ranging from tangrams to colored pencils and paper. An accompanying app interacts with the accessories through a camera angled towards the toys on the table. The different toys are each compatible with a specific game on the app. The accessory toys pairs with a smartphone via Bluetooth.

Credit: Amazon

Categories: Connected.

Interface(s):	Permissions Requested (Android M):
• App (iOS)	App only available on iOS 10.[3]

18. Playmation by The Walt Disney Company

Privacy Policy:

Playmation links to two different privacy policies, one specifically for Playmation, http://www.playmation.com/privacy, and one that applies to Disney apps in general, https://disneyprivacycenter.com/privacy-policy-translations/english.

Credit: Best Buy

Description: Playmation is a set of physical objects including wearable devices, smart figures, and a power activator. Playmation objects pair with a smartphone and may pair with each other via Bluetooth.

Categories: Connected; Smart.

Interface(s):	Permissions Requested (Android M):
• App (Android and iOS)	**Location** Approximate location (network-based) **Storage** Modify or delete SD card contents. Read content on SD card **Other** Full network access, Google Play license check, prevent phone from sleeping, Google Play billing service, pair with Bluetooth devices, access Bluetooth settings, view network connections, view Wi-Fi connections

[3] *See* note 1.

19. Pokemon GO Plus by The Pokemon Company

Privacy Policy:

Pokemon GO Plus links to a policy given by Pokemon, http://www.pokemon.com/us/privacy-policy/, but in terms of the data collected, the policy given by Niantec, the app developer, also applies, https://www.nianticlabs.com/privacy/pokemongo/en/.

Credit: Nintendo

Description: Pokemon GO Plus is a wearable bracelet that allows users to play an app game passively without accessing the app directly. The app has to have been downloaded onto a smartphone in order for the toy to function. It pairs with a smartphone via Bluetooth.

Categories: Connected.

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**Camera** Take pictures and videos **Contacts** Find accounts on the device **Location** Approximate location (network-based), precise location (GPS and network-based) **Storage** Modify or delete SD card contents. Read content on SD card **Other** Activity recognition, prevent phone from sleeping, receive data from Internet, access Bluetooth settings, control vibration, view network connections, full network access, Google Play billing service, pair with Bluetooth devices

20. SelfieMic by Starmaker Interactive

Privacy Policy: http://www.starmakerstudios.com/web/privacy

Description: SelfieMic is a physical microphone that is attached to a selfie stick that attaches to a smartphone. An app must be downloaded onto the smartphone, which acts like a karaoke machine. The physical microphone connects to the app via Bluetooth and records voice and video onto the app.

Categories: Connected.

Credit: Amazon

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**Camera** Take pictures and videos **Contacts** Read your contacts **Microphone** Record audio **Phone** Read phone status and identity, reroute outgoing calls, directly call phone numbers **SMS** Receive text messages (SMS), read your text messages (SMS or MMS) **Storage** Modify or delete SD card contents, read content on SD card **Other** Draw over other apps, prevent phone from sleeping, receive data from Internet, view network connections, full network access, retrieve running apps, Google Play billing service, view Wi-Fi connections

21. Sky Viper Camera Drone Quadcopter by Skyrocket Toys

Description: Sky Viper Camera Drone Quadcopter is a camera drone that can take pictures and videos. It does not connect to the internet or to any devices via Bluetooth or otherwise. A child can use the drone to film video and then a cable to download the video onto a computer. The toy, however, cannot connect share data with other devices via the Internet or Bluetooth and live streaming of video is not available.

Categories: Non-connected.

Credit: Amazon

22. Smart Toy by Fischer-Price, Inc.

Privacy Policy: http://smarttoy.com/privacy

Description: Smart Toy are stuffed animals that act as a companion and play games with or without connecting to the Internet or to an accompanying app via Bluetooth. It comes with cards that can be shown to its camera and induce certain games and activities. An accompanying app, that pairs to the toy via Wi-Fi or Bluetooth, also allows users to control the games and activities.

Categories: Connected; Smart.

Credit: Toys "R" Us, Inc.

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS)	**Location** Approximate location (network-based) **Other** Full network access, pair with Bluetooth devices, connect and disconnect from Wi-Fi, access Bluetooth settings, view network connection, view Wi-Fi-connections

23. Sphero Star Wars BB-8 by Sphero Inc.

Privacy Policy: http://www.sphero.com/privacy

Description: Sphero Star Wars BB-8 is a spherical robot with a free-moving domed head. It can be purchased along with an accompanying wrist band that allows users to control the robot through movements and gestures. The robot pairs with a smartphone through Bluetooth.

Categories: Connected.

Credit: Amazon

Interface(s):	**Permissions Requested (Android M):**
• App (Android and iOS) • Wrist Band control remote	**Location** Uses the device's location **Photos/Media/Files** Uses one or more of: files on the device, such as images, videos, or audio; the device's external storage **Camera** Uses the device's camera(s) **Microphone** Uses the device's microphone(s) **Wi-Fi connection information** Allows the app to view information about Wi-Fi networking, such as whether WiFi is enabled and names of connected Wi-Fi devices **Bluetooth connection** Allows the app to control Bluetooth, including broadcasting to or getting information about nearby Bluetooth devices. **Device ID & call information** Allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call

24. Tamagotchi by BanDai Co., Ltd.

Description: Released in 1996, Tamagotchi is a virtual pet that has its own personality and makes its own choices. Today, Tamagotchi pets are able to connect and make more complex decisions.

Categories: Non-connected.

Credit: Tamagotchi Digital Friends

25. Teenage Mutant Ninja Turtles Talk-to-Me Mikey by Playmates Toys

Description: Talk-to-Me Mikey is a physical turtle figure that has preset answers to specific voice-recognized questions. It does not connect to the internet or to any devices. Though it can recognize speech, it only reacts to preset questions.

Categories: Non-connected; Smart.

Credit: Toys "R" Us, Inc.

26. Wiggy by Spiral Toys, Inc.

Description: Wiggy is a piggy bank that calculates how much money is being saved. Through an accompanying app, parents can send digital money to their children. Spiral Toys, the manufacturer, is currently developing an accompanying card that would allow parents to send their children real money transferred through bank accounts. It pairs with a smartphone through Bluetooth.

Categories: Connected.

Credit: Spiral Toys, Inc.

Interface(s):	**Permissions Requested (Android M):**
• App (iOS)	App only available on iOS 10.[4]

[4] *See* note 1.

KIDS & THE CONNECTED HOME: PRIVACY IN THE AGE OF CONNECTED DOLLS, TALKING DINOSAURS, AND BATTLING ROBOTS

DECEMBER 2016