Smart Decisions about Smart Toys

High-tech toys can put children at risk

U.S. PIRG Education Fund

Smart Decisions about Smart Toys

High-tech toys can put children at risk

U.S. PIRG EDUCATION FUND

WRITTEN BY:

R.J. CROSS
U.S. PIRG Education Fund

December 2022

Acknowledgments

U.S. PIRG Education Fund would like to thank our donors for supporting our work on consumer protection and public health issues.

The author wishes to thank Rachel Franz at Fairplay and Katharina Kopp at the Center for Digital Democracy for their insights and suggestions.

Thanks also to Teresa Murray, U.S. PIRG's Consumer Watchdog, for her editorial support.

The author bears responsibility for any factual errors. Policy recommendations are those of U.S. PIRG Education Fund. The views expressed in this report are those of the author and do not necessarily reflect the views of our funders or those who provided review.

With public debate around important issues often dominated by special interests pursuing their own narrow agendas, U.S. PIRG Education Fund offers an independent voice that works on behalf of the public interest. U.S. PIRG Education Fund, a 501(c)3 organization, works to protect consumers and promote good government. We investigate problems, craft solutions, educate the public and offer meaningful opportunities for civic participation. For more information about U.S. PIRG Education Fund or for additional copies of this report, please visit www.uspirgedfund.org.

Design: R.J. Cross
Cover image: PxHere license, CC0 Public Domain.

Table of Contents

Executive Summary

EVERY YEAR, MORE HIGH-TECH toys are hitting the market. Connected and smart toys include technology like an internet connection or artificial intelligence software that learns about your child and personalizes play.

These toys can offer features parents and kids may want, but **smart toys bring news types of risk:**

- *Data collection* - Smart toys can collect significant data about children. For example, the manufacturer of the software for the Fuzzible Friends Alexa-connected toy states in its privacy policy that it may receive transcripts of a child's interactions with the toy, contingent on parental consent.

  Smart toys may store data about children on company servers, and may partner with other firms to process and store data. They may reserve the right to share your child's data with other parties, including third-party marketers. Over time, your child may unwittingly disclose a lot of information in conversations with their digital companion. The UN has warned that companies could use this data to classify children in buckets, and that long-term storage of information leaves open the possibility that companies may commercialize it in the future, selling it to other parties that may want it, for example, to determine a child's future educational opportunities.

- *Breaches and hacks* - The more data a company gathers on your child, and the more companies it shares it with, the more likely your child's information is to be subject to a breach. In 2015, the largest ever hack of kids' information exposed the names, birthdays, genders and in some cases photos and recordings of 6.4 million children.

- *Microphones and cameras* - If hacked, connected toys can be used to eavesdrop on kids. A conversational doll, My Friend Cayla, had an unsecured Bluetooth connection, enabling the doll to become a microphone for anyone nearby to talk to a child through. The FBI has warned parents that toys with microphones may collect conversations that happen within earshot, even when a toy isn't being played with.

- *Inappropriate content* - Toys with a companion website where kids can download content from other users can lack safeguards for age-appropriateness. In 2019, researchers successfully uploaded content with swearing on one such kids platform.

- *In-app purchases* - Apps can use deceptive tricks to nudge kids to make unsupervised in-app purchases, such as having favorite characters encourage paid-for upgrades. One 6-year-old spent over $16,000 before his parents realized.

- *Marketing to your child* - Smart toys can use "stealth marketing" touting brands and products to your child. Using trusted fictional characters makes it hard for kids to understand they're interacting with an ad. Smart toys can also log your child's preferences over time, and could potentially make that data available to advertisers. The ad industry invests heavily in advertising to kids. An industry trade report suggested marketing can be done to kids as young as age 3.

- *Childhood development* - Researchers have raised that conversational smart toys may negatively impact young children's language development and social skills.

The market for smart toys is growing rapidly. Smart toy revenue is forecasted to reach $18 billion by 2023 - a nearly 200% increase from 2018.

A full tips guide for parents considering buying a smart toy is included at the end of the report.

Tips for parents include:

1) **Research the toy's potential safety risks before buying.** Does the manufacturer have any history of privacy violations?
2) **Understand all the toy's features.** Microphones, cameras, in-app purchases or chat functions can make toys riskier.
3) **Look for toys with a physical component to connect it to the internet.** Hackers can compromise toys that use unsecured Bluetooth connections.
4) **Supervise playtime, especially with younger kids.** Be sure these toys are used in shared spaces, instead of children's bedrooms.
5) **Read the fine print.** Make sure you understand what data the toy collects, what companies may get that data, and that you can ask the company to delete any data it has on your child. This report includes an entire section on "how to read the fine print".

Introduction

LIFE HAS BECOME increasingly digital, and that includes the toys our children play with. Electronic toys have become common in the marketplace, and they increasingly include technology like internet connections or artificial intelligence software that learns about your child and personalizes play.

Every year, more high-tech toys are hitting the market. Smart toy revenue is forecasted to reach $18 billion by 2023 - a nearly 200% increase from 2018.[1]

These toys can offer features parents and kids many want, but they also bring new types of risk. Given their rapidly growing popularity, now is the time for parents to think carefully about whether to bring these toys into the home, and if so, how to do it safely.

Here we catalog some of the risks of internet-connected and high-tech toys, and offer tips for parents to help make smart decisions about smart toys.

What are connected and smart toys?

CONNECTED TOYS USE WiFi or Bluetooth to deliver a part or all of their play functions. Just as connecting to the internet gives a laptop access to a huge number of uses - like allowing you to stream video, download apps, or check email - an internet connection gives toys a wider range of capabilities. In addition, smart toys are those that include some element of artificial intelligence (AI) that learns about your child and personalizes play over time. Common types of connected and smart toys include dolls, robots and interactive games.

WiFi or Bluetooth connections are often added to toys to make smart toys more interactive. An internet connection enables many to be used with a companion app, giving your kid a digital interface for interacting with their toy. These apps, for example, can serve as a kind of "remote control," allowing a child to use an app to control the toy's movement in the physical world, or teach it to perform multi-step tricks.[2] Others may enable augmented

[1] Juniper Research, "Smart Toy Revenues to Grow by Almost 200% from 2018 to $18 billion by 2023" *(press release)*, 8 May 2018. Available at: https://www.juniperresearch.com/press/smart-toy-revenues-grow-almost-200pc-by-2023.

[2] For examples of connected toys with these features, see: https://www.pocket-lint.com/parenting/buyers-guides

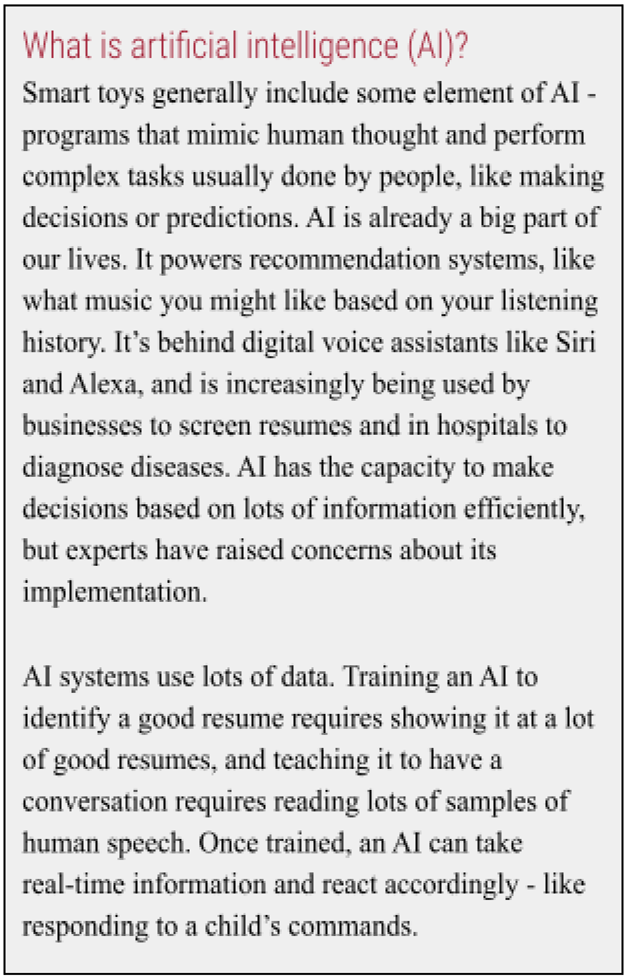
reality features - incorporating a physical toy into a digital landscape that’s viewable on a tablet or screen.

Smart toys often include other technologies such as microphones, cameras or sensors in conjunction with an internet connection to enable all their features. Many can transmit data to apps or outside servers that is then processed and used to prompt the toy to act accordingly.

For example, some dolls that have conversations with kids have a microphone, and use WiFi to transmit a child’s words to speech recognition software maintained by the manufacturer. Then, the child’s words may be compared against databases of possible responses for the doll to deliver, which the company then transmits to the doll’s microphone over WiFi. In some cases, your child’s answers may be kept over the longer term, enabling the doll to remember, for example, your child’s name or favorite animal.[3]

Other smart toys have “onboard electronics” like microprocessors and storage capabilities built into the toy itself. These can include additional features like facial recognition, and sensors that can detect light, touch, temperature and proximity.[4] These can serve to give toys particularly lifelike features, like appearing to shiver when it’s cold or fall asleep when the lights are turned off.

Smart toys are currently being manufactured for all age groups - infants, toddlers, preschoolers, and school age children.



What is artificial intelligence (AI)?

Smart toys generally include some element of AI - programs that mimic human thought and perform complex tasks usually done by people, like making decisions or predictions. AI is already a big part of our lives. It powers recommendation systems, like what music you might like based on your listening history. It’s behind digital voice assistants like Siri and Alexa, and is increasingly being used by businesses to screen resumes and in hospitals to diagnose diseases. AI has the capacity to make decisions based on lots of information efficiently, but experts have raised concerns about its implementation.

AI systems use lots of data. Training an AI to identify a good resume requires showing it at a lot of good resumes, and teaching it to have a conversation requires reading lots of samples of human speech. Once trained, an AI can take real-time information and react accordingly - like responding to a child’s commands.

/142793-best-tech-toys-connected-toys-robots-and-more

[3] American Library Association, “Connected Toys” *(webpage)*, accessed on 10 November 2022 at: https://www.ala.org/tools/future/trends/connectedtoys.

[4] See for example: “KD Group's 'My Loopy' Uses AI and Sensors to Interact with Kids” *(webpage)*, TrendHunter, 6 March 2018. Available at: https://www.trendhunter.com/trends/my-loopy.

The potential of smart toys

THE PREVALENCE OF SMART and connected toys available for sale has grown in recent years, thanks to a number of factors in the broader marketplace, including developments in new smart technology, the increased presence of screens, smartphones and tablets in children's lives, and the wider adoption of Internet of Things devices, like smart appliances, in people's homes.[5]

Parents may want connected toys to offer features like generating reports about a child's engagement that can help understand their child's development in new ways, or potentially keeping kids' interest longer than analog toys with software updates. Other parents appreciate that some smart toys are interactive without increasing their child's screen time. Some toys purport to offer educational benefits, like teaching a child vocabulary in a second language, or teaching them the basics of coding and robotics.

According to the advocacy group Fairplay, many of these positive claims made by manufacturers and marketers of smart toys have not been verified by outside experts.[6] Smart toys also come with potentially serious risks that should be considered carefully before bringing them into the home.

[5] See note 3.

[6] Fairplay, "Connected Toys and Devices - Safe, Secure, & Smart Guide to Choosing Tech for Your Preschooler" *(webpage)*, accessed on 6 November 2022. Available at: https://fairplayforkids.org/pf/safe-secure-smart-toys/.

Smart toys can collect, store and use a lot of data about children

CONNECTED AND SMART TOYS can require the collection of your child’s data to function. Under the Children’s Online Privacy Protection Act (COPPA), companies cannot collect personal information from children under 13 without parental consent. It’s possible, however, that “giving consent” could be as simple as turning the toy on.[7] It’s easy to misunderstand the full implications of giving consent for data collection during play.

Data collected can include the information provided by a parent while registering the toy, or a catalog of a child’s performance or behavior when playing with a toy. Some toys are focused on creating a relationship with your child[8], meaning they want to find out and remember things like your child’s name, favorite animal, and other content of past conversations. Relationship-centric, conversational toys may also solicit information from kids about other members of the household, or about visitors.[9] “Remembering” all this information so the toy can revisit it with your child means that data is stored somewhere - usually on a company’s servers.

Smart toy manufacturers may partner with other companies, like data analytics firms, in order to process and store data.[10] They may also reserve the right to transmit data to other actors as well, meaning your child’s personal information could potentially get shared with a broad number of companies, including third party marketers - especially when the company fails to provide a specific list of what parties may receive your child’s data in its privacy policies.[11] The data gathered about your child may become the intellectual property of these

[7] This is similar to what some app developers do - in some cases, giving consent for data collection is as simple as downloading an app. See: *CoPIRG comments on Colorado Privacy Act rulemaking*, available at: https://pirg.org/resources/copirg-comments-on-colorado-privacy-act-rulemaking/.

[8] “Smart toys and wearable gadgets: buying tips for parents” *(webpage)*, Internet Matters, accessed on 6 November 2022 at: https://www.internetmatters.org/resources/tech-guide/smart-toys-and-wearable-gadgets/#toys.

[9] Valerie Steeves, *A dialogic analysis of Hello Barbie’s conversations with children*, Big Data & Society, 29 April 2020. Available at: https://journals.sagepub.com/doi/full/10.1177/2053951720919151.

[10] Karen Louise Smith and Leslie Regan Shade, *Children’s digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture*, Big Data & Society, 26 October 2018. Available at: https://journals.sagepub.com/doi/10.1177/2053951718805214.

[11] Ibid.

companies.[12] Some of your child's data may even go towards training different AI systems.[13]

In general, companies have the incentive to gather more data about children than is needed, and use that data for secondary commercial purposes, like building profiles of a child's interests that can be used to target them with ads.[14] As documented by the Center for Digital Democracy, marketing companies have published reports about the profitability of marketing to children, who often heavily influence how families spend their money.[15] For more on marketing to children, see page 15.

Companies that collect data on children could save it for long periods of time, and potentially commercialize it in the future by selling it to third parties. This could have big impacts on children's lives. The UN has warned, for example, that a toy company that collects intimate data on kids from an early age could potentially sell it to colleges and universities who might want such data for admissions decisions.[16] AI may use data from toys to classify children in buckets based on various metrics like attention span or learning pace.

Smart toys that have two-way conversations with your child may store recordings or transcripts.

One common type of smart toy is dolls or stuffed animals that have active conversations with kids. The companies behind these toys may be gathering detailed logs of everything your child says.

Two-way conversational smart toys often utilize artificial intelligence and speech recognition software to take a recording of a child, turn it into a transcript, analyze it, and prompt the toy to respond in a conversational manner - usually soliciting more interaction and information from the child. Some conversational smart toys include a microphone and use WiFi to access speech recognition software, as was the case with Mattel's Hello Barbie doll that was introduced in 2015 and

[12] See note 9.

[13] World Economic Forum, "Our children are growing up with AI. Here's what you need to know" *(article)*, 28 January 2022. Available at: https://www.weforum.org/agenda/2022/01/artificial-intelligence-children-technology/.

[14] Mikaela Cohen, "Future AI toys could be smarter than parents, but a lot less protective", *CNBC*, 11 July 2022, available at: https://www.cnbc.com/2021/07/11/future-ai-toys-may-be-smarter-than-parents-and-less-protective.html.

[15] *Comments of Center for Digital Democracy et al to the Federal Trade Commission regarding commercial surveillance rulemaking*, November 2022, available at: https://fairplayforkids.org/wp-content/uploads/2022/11/ANPRM_comments.pdf.

[16] World Economic Forum, "Smart toys: Your child's best friend or a creepy surveillance tool?" *(article)*, 31 March 2022. Available at: https://www.weforum.org/agenda/2021/03/smart-toys-your-child-s-best-friend-or-a-creepy-surveillance-tool/.

later discontinued.[17] Other conversational toys piggyback off of the technology of voice assistants like Amazon's Alexa, and use a connection with a smart home speaker to communicate with a child instead of incorporating a microphone into the toy itself.

In 2021, a Mozilla Foundation review of the Fuzzible Friends Alexa-connected toy found that the manufacturer of the software that enables the plush toy to talk receives information about a child in the course of play.[18] A 2022 review of these privacy policies by U.S. PIRG Education Fund researchers found the same concerns remain.

Creativity Inc., the company that created the Alexa Skill software that makes Fuzzible Friends interactive, can receive a child's personal data from Amazon, contingent on the parental consent given to Amazon.[19] This means the company may receive a lot of information, including geolocation information and transcripts of a child's conversations with their digital companion.[20] The company gives the example that if a user were to state their age during a session using their services, then that would be included in the transcript.[21] The company states these transcripts are anonymized, but it's still a lot of information for a company to have, and there's no good reason for a company to have this level of detailed data. At the time of this report's publication, Fuzzible Friends are available for purchase from Walmart, eBay, Amazon and other retailers.

Of all smart toys, ones that have free-flowing conversations with your child have the potential to lead to excessive data collection in particular. Children likely come to view the toy as a trusted friend, and may unwittingly disclose a lot of personal information in the course of conversations, not realizing behind the toy are companies that are the ones doing the listening and the talking.

Unclear terms and conditions can leave parents in the dark.

Terms and conditions and privacy policies are notorious for being long and difficult to read. A 2016 study by the Norwegian Consumer Council found that if the average person read the entirety of every privacy policy they signed in a year, they'd have to read

[17] James Vlahos, "Barbie Wants to Get to Know Your Child", *The New York Times Magazine,* 16 September 2015. Available at: https://www.nytimes.com/2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html?_r=0.

[18] Mozilla Foundation, "Fuzzible Friends Alexa Connected Toy", 2021. Available at: https://foundation.mozilla.org/en/privacynotincluded/fuzzible-friends-alexa-connected-toy/.

[19] See: Creativity Incorporated's privacy policy. Archived on December 2, 2022: Source: https://web.archive.org/web/20221202220511/http://www.creativityinc.com/privacy-policy.

[20] Ibid.

[21] Ibid.

250,000 words of fine print - which is longer than the New Testament, and would take over 24 hours to read out loud.[22]

The fine print of all the products we use is often hard to parse and can be surprisingly vague. For example, it's common to see companies reserve the right to share your data with classes of companies like "service providers" or "partners", without giving a full list of who exactly that entails. If specific companies are named, usually the privacy policy refers you to the privacy policies of those companies, meaning you may have to read even more fine print to fully understand what's going on.

This is the case for many technology companies, and unfortunately, it can be the case for toy manufacturers, too. Anytime a parent comes away confused after looking at the fine print, it's better to move on and find a different toy made by a company that takes the security of children seriously enough to put forward a clear privacy policy.

For tips on what to look for in the fine print, see page 20.

The potential risks of smart toys

SMART TOYS CAN POSE RISKS to child security, privacy, and development.

Microphones, cameras and sensors can pose safety concerns.

Many web-enabled toys include devices like microphones or cameras that can pose security risks to children. If hacked, these toys can be used to eavesdrop on or even communicate with kids. The FBI has issued warnings about connected toys, advising that consumers should consider cybersecurity risks before bringing them into the home.[23]

In 2017, U.S. PIRG Education Fund reported that the My Friend Cayla doll had an unsecured Bluetooth connection, enabling Cayla to become a microphone for anyone nearby to talk to a child through the doll. Smartphones automatically recognized the doll as a normal hands-free headset, and did not require a password to connect to the doll, or for a person to physically

[22] Øyvind H. Kaldestad of the Norwegian Consumer Council, "250,000 words of app terms and conditions", 2016, available at: https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/.

[23] Federal Bureau of Investigations, "Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children" *(public service announcement)*, 17 July 2017. Available at: https://www.ic3.gov/Media/Y2017/PSA170717.

interact with the doll at all in order to use it to converse with children.[24] In 2017, German officials ordered parents to destroy the dolls, citing concerns that they may be used to illegally spy on kids.[25]

In 2021, the U.S. PIRG Education Fund found a similar security problem with The Singing Machine, a Bluetooth karaoke microphone that allowed users to connect it with any app or music platform. The microphone didn't require a PIN or other verification to connect to the device via Bluetooth. PIRG toy researchers were able to connect to The Singing Machine from outside of their home at about 30 feet away. A bad actor could connect to the device and play anything from an explicit song to a voice recording telling a child to come outside.[26]

Other concerns raised by the FBI include the possibility that toys with microphones may collect conversations that happen within earshot even when direct play with a toy isn't occurring, and that the risk of child identity theft rises due to the amount of information children may unwittingly disclose to their internet-connected friend.[27] The agency also warned that some connected toys may collect GPS location history or WiFi network information.

Breaches and hacks can expose children's data.

Internet-connected toys often collect data about children as they play. The more data companies collect on users, the more likely that data will be subject to breach or hack, and smart toys are no exception.

In 2015, for example, the toy company VTech was the target of a successful cyber attack that exposed the data of at least 6.4 million children – the largest ever hack of kids' information to date.[28] The exposed data included children's names, birthdays, and genders, and in some cases, photos, recordings and chat logs.[29] This episode is far from an isolated incident.

[24] Dev Gowda and Ed Mierzwinski, U.S. PIRG Education Fund, *Trouble in Toyland: The 32nd Annual Survey of Toy Safety*, November 2017. Available at: https://publicinterestnetwork.org/wp-content/uploads/2017/11/USP-Toyland-Report-Nov17-Web.pdf.

[25] Philip Oltermann, "German parents told to destroy doll that can spy on children", *The Guardian*, 17 February 2017. Available at: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children.

[26] U.S. PIRG Education Fund, Trouble in Toyland: 36th Annual Toy Safety Report, November 2021. Available at: https://pirg.org/wp-content/uploads/2021/10/PIRG_Trouble-In-Toyland_2021.pdf.

[27] See note 23.

[28] "VTech hack: Data of 6.4M kids exposed", *CNBC*, 2 December 2015. Available at: https://www.cnbc.com/2015/12/02/vtech-hack-data-of-64m-kids-exposed.html.

[29] Lorenzo Franceschi-Bicchierai, "Hacker Obtained Children's Headshots and Chatlogs From Toymaker VTech", *Motherboard*, 30 November 2015, Available at: https://www.vice.com/en/article/yp3zev/hacker-obtained-childrens-headshots-and-chatlogs-from-toymaker-vtech.

Another example, from 2017, involved CloudPets internet-enabled stuffed animals, which were designed to exchange recorded messages between kids and parents (useful, for example, while a parent is on a business trip). The toys exposed the emails and passwords of more than 800,000 accounts, and made it possible for outside actors to access more than 2 million of the recorded messages between children and their parents online.[30] Major toy retailers stopped selling the stuffed animals by June 2018 — including eBay — but in 2021, PIRG Education Fund researchers found them still for sale from certain retailers on eBay.[31]

Platforms may include inappropriate content for download.

Some connected toys have a companion online platform or app. In some cases, these allow children to download content that is created by other users, rather than the manufacturer itself. Through these sites and apps, children can interact with content that may not have been screened to make sure it's age appropriate.

In 2019, the non-profit Which? and the cybersecurity firm NCC Group found toys where users could upload inappropriate content to companion web portals. For example, a build-your-own video game that teaches kids basic coding skills, Bloxels, has an online arcade where users can upload their designed games. Researchers were able to upload a game that featured swearing and make it available to all other users.[32]

Add-on sales and in-app purchases can cost parents money.

Smart toys can end up costing parents more money than expected. Some smart toys may come with a monthly subscription cost to get updates or access new features, in addition to the upfront cost of the toy.

Another concern is in-app purchases in games tailored for kids, enabling children to accidentally spend money unsupervised. A 2020 survey found that 40% of parents reported that their children spend up to $10 a month on in-app purchases, while over 8% said it's over $100 monthly.[33]

[30] Lorenzo Franceschi-Bicchierai, "Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings", *Motherboard*, 27 February 2017. Available at: https://www.vice.com/en/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings.

[31] See note 26.

[32] Andrew Laughlin, "Kids' karaoke machines and smart toys from Mattel and Vtech among those found to have security" *(article)*, Which?, 10 December 2019. Available at: https://www.which.co.uk/news/article/kids-karaoke-machines-and-smart-toys-from-mattel-and-vtech-among-those-found-to-have-security-flaws-in-a-which-investigation-aCZvy9z0N7R2.

[33] "The Hidden Costs Of Free Kids Apps And Games For Parents" *(article)*, School Holidays 4 May 2022, available at: https://schoolholidays.com.au/blog/the-hidden-costs-of-free-kids-apps-and-games-for-parents.

This can be particularly problematic for young children who likely don't understand all the implications of spending money. A 2019 study found that 95% of the most-downloaded free apps for kids under age 5 feature ads, and that some even featured characters encouraging in-app purchases.[34] One 6-year old accidentally spent over $16,000 inside a tablet game, in part because the button for in-app purchases was the game's main character, making the invitation to spend money friendly and more appealing for a child. Some of the items available for purchase cost as much as $99.99.[35]

Data gathered on children may be used for marketing.

Advertising to children is a concern for many parents, and connected toys have created new opportunities for advertising to children.

Some connected toys with companion apps or associated websites may feature ads designed to target children of specific ages. In an industry report by the trade group the Internet Advertising Bureau, it advises: "if a user is currently playing a racing game with animated content and requires an early education reading level, then you can contextually target an ad intended for a boy between the ages of 6 to 8." The report goes on to suggest advertising can target ads to age groups as young as 3-5 year olds.[36]

Other advertising practices targeting kids are harder to identify. Some connected toys can come pre-programmed with phrases touting certain products or brands to your child. This practice is known as "embedded advertising" or "stealth marketing."[37] In the case of the My Friend Cayla doll, she was pre-programmed to discuss her favorite Disney movies with children. The company that manufactured Cayla, Genesis Toys, had a commercial relationship with Disney that wasn't

[34] See: Marisa Meyer et al, Advertising in Young Children's Apps: A Content Analysis, *Journal of Developmental & Behavioral Pediatric*s: January 2019 - Volume 40 - Issue 1. Available at: https://journals.lww.com/jrnldbp/Abstract/2019/01000/Advertising_in_Young_Children_s_Apps__A_Content.4.aspx; and: Jenny Radesky, MD et al, Digital Advertising to Children *(policy statement)*, The American Academy of Pediatrics, 1 July 2020. Available at: https://publications.aap.org/pediatrics/article/146/1/e20201681/37013/Digital-Advertising-to-Children?

[35] Malcolm Owen, "Child spends $16K on iPad game in-app purchases", *Apple Insider*, 13 December 2020. Available at: https://appleinsider.com/articles/20/12/13/kid-spends-16k-on-in-app-purchases-for-ipad-game-sonic-forces.

[36] Internet Advertising Bureau, *Guide to Navigating COPPA: Recommendations for compliance in an increasingly regulated children's media environment,* October 2019. Archived on 29 November 2022 at: https://web.archive.org/web/20220720020013/https://www.iab.com/wp-content/uploads/2019/10/IAB_2019-10-09_Navigating-COPPA-Guide.pdf.

[37] *Comments of Fairplay et al to Federal Trade Commission in the Matter of Protecting Kids from Stealth Advertising in Digital Media*, July 2022. Available at: https://fairplayforkids.org/wp-content/uploads/2022/07/influencer-comments.pdf.

obvious.[38] Using trusted fictional characters to advertise to kids can seem like they're getting "authentic" communications from a trusted friend, rather than an advertisement.[39] In 2022, the advocacy group Fairplay, along with other groups including U.S. PIRG, submitted a report to the Federal Trade Commission petitioning for action on stealth marketing to kids as an unfair and deceptive trade practice.[40]

Some researchers and advocates have raised particular concerns about interactive, conversational toys creating digital profiles of children to log their likes and dislikes, as well to elicit information about a child's family and their interests.[41] In general, the creation of digital profiles cataloging demographic and interest information about individuals is the primary vehicle for today's online targeted advertising systems.[42] While COPPA puts significant controls in to limit the collection and sharing of children's data under age 13, COPPA doesn't ban targeted advertising to kids.[43] A study found that by the time a child turns 13, advertising technology companies have gathered, on average, 72 million data points about them.[44] Given that at least some smart toys reserve the right to share data with third party marketers[45], your child's favorite toy may be contributing to the digital profile constructed on your child that's sold to many companies.

Some smart toys may hinder the development of young children.

Play is crucial for child development - it helps build cognitive, physical, social and emotional skills in young children.[46] Increasingly, researchers have raised potential harms that smart toys may inflict on young kids' development.

Language development

Smart toys can impact language development. For example, preschoolers often have to work through communication problems with peers

[38] "Connected toys violate European consumer law" *(press release)*, Norwegian Consumer Council, 6 December 2016. Available at: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/.

[39] See note 37.

[40] Ibid.

[41] See, for example, the sources in notes 9 and 14.

[42] R.J. Cross, "Cookie pop-ups: why you should think twice before hitting "accept" *(article)*, U.S. PIRG, 19 July 2022. Available at: https://pirg.org/articles/cookie-pop-ups-why-you-should-think-twice-hitting-accept/.

[43] Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" *(webpage)*, accessed on 10 November 2022. Available at: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

[44] Andrew Simms, "The advertising industry is fuelling climate disaster, and it's getting away with it" *(opinion)*, 11 October 2021. Available at: https://www.theguardian.com/commentisfree/2021/oct/11/advertising-industry-fuelling-climate-disaster-consumption.

[45] See note 10.

[46] Aleeya Healey et al, "Selecting Appropriate Toys for Young Children in the Digital Era", *The American Academy of Pediatrics*, January 2019. Available at: https://publications.aap.org/pediatrics/article/143/1/e20183348/37330/Selecting-Appropriate-Toys-for-Young-Children-in?

and adults in order to learn how to express their thoughts coherently - an important life skill.[47] Conversational smart toys lack the ability to work through communication breakdowns, which can particularly frustrate 3 and 4 year olds.[48] Conversational toys might even cut children off while they're in the process of forming their ideas into sentences.[49] It's best to stay away from conversational toys and smart speakers for young children.

Creativity

Researchers have raised the possibility that smart toys may impact children's creativity. When playing with a normal, analog doll or stuffed animal, the child sets the agenda for play and has to invent both sides of the conversation. By contrast, smart toys tend to be the ones directing the play and conversations based on their programmed abilities.[50] With analog toys, playtime is a blank slate. With smart toys, play is restricted to the toys' limitations.

Social skills and relationships

Preschoolers learn best from real-life interactions.[51] This can get complicated when smart toys are in the mix.

Smart toys often have a focus on actively creating a relationship with your child.[52] They are often designed to have "personalities", and emulate emotions. Many advertise that they aim to "bond with your child" and provide companionship.[53] Sometimes toys are programmed to deepen emotional relationships by learning specifics about your child and hyper-personalizing play.[54]

Smart toys, however, are still just toys that happen to have computers inside them. They aren't capable of building reciprocal relationships, trust, or patient and loving friendships. But because they're very good at emulating these traits, and can talk back to children, kids may build a connection with smart toys like they do with people, and attribute emotions and intent to their toys in a different way than they do with analog toys.[55] According to some researchers, this can stunt emotional growth about

[47] Fairplay, "Connected Toys and Devices - Safe, Secure, & Smart Guide to Choosing Tech for Your Preschooler" *(webpage)*, accessed on 6 November 2022. Available at: https://fairplayforkids.org/pf/safe-secure-smart-toys/.

[48] Stefania Druga et al, "'Hey Google is it OK if I eat you?' Initial Explorations in Child-Agent Interaction", *MIT Media Lab*, 2017. Available at: https://robots.media.mit.edu/wp-content/uploads/sites/7/2017/06/idcwp0180-drugaACR.pdf.

[49] See note 47.

[50] See note 9.

[51] See note 47.

[52] "Smart toys and wearable gadgets: buying tips for parents" *(webpage)*, Internet Matters, accessed on 6 November 2022 at: https://www.internetmatters.org/resources/tech-guide/smart-toys-and-wearable-gadgets/#toys.

[53] See for example: https://www.trendhunter.com/trends/interactive-robots.

[54] See note 9.

[55] See note 48.

the ideas of what friendship should look like. As MIT professor Dr. Sherry Turkle, researcher and author of multiple books about children and technology, said in a recent interview with *The Atlantic*: "Pretend empathy does not do the job." Any chance that a child develops a relationship with a smart toy that crowds out building relationships with family or peers means you could end up with "children growing up without the equipment for empathic connection. You can't learn it from a machine."[56]

Interacting with smart toys can also alter the way children interact with real people. In a 2017 study of a group of children's interactions with smart toys, the children recognized that two of the smart toys often fell into repetitive loops, using the same phrases over and over when the toy couldn't understand or respond to a question posed by the children. One parent followed up with researchers after the study to report that her child had started using one of the toy's same repetitive phrases with her father when she didn't want to do what he asked of her.[57]

Conclusion

SMART TOYS, LIKE ANY OTHER technology are not inherently good or bad - it's the way we decide to design and implement them that makes all the difference. Without policy reform, however, it's more likely smart toys will become data collection devices for harvesting the data of children.

It's concerning that, right now, there's very little governance over smart toy manufacturers and their products.[58] Policymakers should institute more oversight over the industry. They should also institute a data minimization policy, requiring companies to only collect the data that's needed to provide the service a consumer is expecting to get, and nothing else.

Policymakers should also ban the collection of children's data for targeted or behavioral advertising. Banning this practice will help cut down on the amount of data collected by companies, and the number of companies this data is shared with.

[56] Alexis C. Madrigal, "Should Children Form Emotional Bonds With Robots?", *The Atlantic*, December 2017. Available at: https://www.theatlantic.com/magazine/archive/2017/12/my-sons-first-robot/544137/.

[57] Emily McReynolds et al, *Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys*, Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, May 2017. Available at: https://dl.acm.org/doi/10.1145/3025453.3025735

[58] World Economic Forum, "Smart Toy Awards: Shaping the Future of Childhood" *(webpage)*, accessed on 6 November 2022. Available at: https://www.smarttoyawards.org/.

Unfortunately, until then, it's on parents to make smart decisions about smart toys. We're here to help.

Smart toy tips for parents

IF YOU ARE THINKING OF buying your child a smart toy, there are steps you should take before bringing it home, and ways to help keep play safe.

Before buying

Make sure the toy is age appropriate - Know what age range the toy is designed for, and understand the reason those recommendations exist. For example, conversational toys and smart speakers aren't good fits for young children developing language skills. That said, each child develops on their own trajectory. By understanding the reasons for age recommendations, you're in a better position to make the right choice for your child.

Research the toy's potential safety risks before buying - Ensure there are no reports of a toy posing known dangers to children. Search the toy manufacturer online to see if there are any news reports or government actions against it for violating privacy standards, and avoid those with a spotty record. Looking up reviews of the toy may also help you identify toys that have made parents feel uncomfortable.

Understand all of the toy's features - Make sure you understand exactly what the toy can do. Consider what features will work best for your family.

Features to consider carefully:

- Cameras, microphones or sensors
- Chat functions
- Location sharing
- In-app purchases
- Level of individual personalization the toy is programmed to accomplish

Features that can be helpful:

- Parental safety controls
- Ability to set time limits
- Ability to turn the toy completely off
- A "touch to talk" feature, so you control when a device is "listening"

Look for toys with a physical component to connect it to the internet - This can even be as simple as having a button on the toy you must press in order to link it to other devices. Ensuring someone must physically interact with the toy helps cut down on the risks of strangers abusing its internet connection. Some toys will require you to enter a password in an app to connect with the toy. This is a good feature to have, but physical requirements are best.

Once a toy has cleared these initial hurdles, the final step is to roll up your sleeves and take a look at the terms & conditions and privacy policy. This is not an easy thing to do, but we're here to help.

How to read the fine print

Reading terms & conditions and privacy policies is hard. It's completely normal to feel intimidated and confused by these documents – they're full of legal lingo and vague statements. If you feel lost or frustrated, just know you're not the only one. We'll walk through the steps together here.

The terms & conditions and privacy policy documents are usually two separate documents – you'll want to find both.

Finding the documents

Typically, you'll find these somewhere on the toy manufacturer's website. A lot of times it'll be at the very bottom of their site with a little link that says "terms and conditions" or "privacy" or "legal information".

If you're having trouble finding these, you can also search the name of the company and "privacy policy" online and see if that helps you.

If you can't find the terms and conditions or privacy policies – and it's possible you might not – it's better to move on and find a different toy made by a different company that's more transparent.

If there are multiple companies involved in delivering the services of a smart toy, you'll want to find terms & conditions and privacy policies for all of them. Sometimes a smart toy manufacturer will partner with outside technology companies to provide elements of the toy's play functions, and these outside companies will have their own policies, and you may find something in that fine print that you don't like. A toy manufacturer's technology providers may be listed in the general information of the toy, in its FAQs, or in the manufacturer's privacy policy (we'll help you find where).

Finding the privacy policies of other companies is particularly important for toys that have a companion website or app you have to download in order to play. Devices like computers, smartphones and tablets are capable of sucking up a lot of unnecessary data, and app developers in general are notorious for collecting children's data illegally. If there's an app, you need to find its policies, too. To find these documents, look at the app's information in the app store. There's often a link to these documents in the app description. If it's not there, try looking at the company's website.

What to look for in the fine print

Once you've found all the documents, it's important for parents to try and find answers to key questions, which we list below. To help find answers, there are some keywords you can search using "ctrl + f" or "command + f" to help navigate – we include these below, too.

1) **Does the toy have a child-specific privacy policy?** Any product designed for children will ideally have a separate children's privacy policy, or at least a section of its privacy policy dedicated to the rights of children. To find it quickly, search the privacy policy and terms & conditions for the word "child". If a child-specific section or document doesn't exist - or you can't easily find it - this is a red flag from the get go.

   Ideally, you'll be able to find the answers to the following questions in that kids-specific document or section.

   Suggested search terms for scanning the fine print: child, minor.

2) **If the toy has a microphone or a camera, is it recording your child's interactions with it? Are those communications transferred anywhere? To whom, and for what purpose?** This data can be sensitive. It's ultimately up to you if you're comfortable with this type of information being collected.

   Suggested search terms: camera, microphone, voice, photo, recording, transcript.

3) **Is the toy collecting any other information about your child, or transferring it to any company that isn't the manufacturer?** Most sensitive is information about your child's location. You want to be pretty careful about who can get this.

   Suggested search terms: location, geolocation.

   Which companies are getting your child's data? Wherever a manufacturer's privacy policy says they're selling, sharing or transferring data to other entities, you want to see the specific names of specific companies. It's not uncommon to see privacy policies or terms & conditions that say "we share your information with service providers" or "third parties" or "business partners" and then give you no clues about who

those entities are. The best toy manufacturers will follow any of these phrases up with specific names of who, exactly, is getting your child's data.
When the company lists out its technology partners or service providers partners explicitly, these are the companies you'll want to find privacy policies for, and figure out what they do with your child's data.

Suggested search terms: data, personal information, transfer, share, sell, third party, third parties, service provider, partner, business.

4) **Does the company retain the right to share your child's data with advertisers?** Any toy that states it can share data with advertisers may be worth staying away from – advertisers tend to have weaker security protocols in place and tend to share data with a lot of other entities. Plus, letting a child see ads that companies have tailored based on what they think a kid will like has been linked with unhealthy habits – like increased cravings for junk food. In a privacy policy, targeted advertising may also be called "interest-based" or "personalized" advertising.

   Suggested search terms: advertiser, advertising, marketing.

5) **Can you request a record of your child's data so you can see what the company has on file? And can you request your child's data be deleted?** You want to maintain some level of control over your kid's information, and having access and deletion rights are some of the most important. You want to be able to delete data if, for example, you have reason to believe your child overshared some sensitive information.
   You'll also want deletion rights for once your child loses interest in or outgrows a toy, so you can make sure the company isn't holding onto information unnecessarily, which can put your kid at risk in case of a data breach or hack, even months or years down the line.

   Suggested search terms: delete, deletion, parental access, personal information rights, your rights.

6) **If there's a data breach, will you be notified?** You want a company that commits to transparent communication about any possibilities that your child's data has been compromised in any way.

   Suggested search terms: security, breach, hack, notify, communication.

7) **Does the company state it is allowed to change the terms & conditions or privacy policy without notifying you?** This can be a red flag if they can make substantive changes – especially when it comes to types of data they collect and who they share it with – without alerting you.

   Suggested search terms: change, revision, revised, edited, notify.

Unfortunately, it's possible after hunting down all the documents and reading the fine print that you won't be able to find the answers to all of these questions in the terms & conditions or privacy policies. These documents can omit important information, like a full list of companies the manufacturer may share your child's data with. If this is the case, it's safer to find a different toy made by a company that takes the security of children more seriously.

Once the smart toy is home

Supervise playtime, especially with younger kids - Establish with your child that playtime with the toy is only with parental supervision. This helps to ensure that if someone is hacking and using the toy to interact with your child, you can take action immediately. Be sure these toys are used in shared spaces, instead of children's bedrooms or the bathroom.

Turn it off - Always turn the toy off when not in use. For younger children, store it in a place your child can't reach when playtime is over to ensure they can't turn it on without supervision, re-enabling the toy to pose unmonitored risks.

Stay on top of security updates - Many web-enabled toys and their companion apps will issue periodic updates. Make sure to stay on top of these.