Toying with Privacy: Regulating the Internet of Toys

ELDAR HABER*

Recently, toys have become more interactive than ever before. The emergence of the Internet of Things *(IoT) makes toys smarter and more communicative: they can now interact with children by "listening" to them and responding accordingly. While there is little doubt that these toys can be highly entertaining for children and even possess social and educational benefits, the* Internet of Toys *(IoToys) raises many concerns. Beyond the fact that IoToys devices might be hacked or simply misused by unauthorized parties, datafication of children by toy conglomerates, various interested parties, and perhaps even their parents could be highly troubling. It could profoundly threaten children's right to privacy by subjecting and normalizing them to ubiquitous surveillance and datafication of their personal information, requests, and any other information they divulge. While American policymakers acknowledged the importance of protecting children's privacy online back in 1998 when crafting Children's Online Privacy Protection Act (COPPA), this regulatory framework might become obsolete in the face of the new privacy risks that arise from IoToys. Do fundamental differences between websites and IoToys necessitate a different legal framework to protect children's privacy? Should policymakers recalibrate the current legal framework to adequately protect the privacy of children who have IoToys devices? Finally, what are the consequences for children's privacy of ubiquitous parental surveillance through IoToys—allegedly granted to safeguard children from online risks? And how might children's privacy be better framed and protected in this context?*

---

* Senior Lecturer, Faculty of Law, University of Haifa; Faculty Member, Haifa Center for Law & Technology (HCLT) and the Center for Cyber Law & Policy (CCLP), University of Haifa; Faculty Associate, Berkman-Klein Center for Internet & Society, Harvard University (2016–2018). I am much grateful to Meryl Alper, Michael Birnhack, Niva Elkin-Koren, Esther Tabitha Earbin, Michal Gal, Natali Helberger, Sunny Kalev, Omri Rachum-Twaig, Arianne Renan Barzilay, Galia Schneebaum, Yoram Shachar, Adam Shinar, Lev Streltsov and Tal Zarsky for their extremely helpful suggestions and comments. I also wish to thank Chen Arobas and Ori Gorali for their excellent assistance in research, and participants of the Haifa law school research seminar (Feb. 2018); GYSM "Legal Rules for the Digital Economy" workshop, Potsdam, Germany (Feb. 2018); Law & Emerging Technology Event at the Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany (Apr. 2018); Faculty seminar at Radzyner Law School at IDC Herzliya (May 2018). This work was supported by the Center for Cyber Law & Policy at the University of Haifa in conjunction with the Israel National Cyber Directorate in the Prime Minister's Office.

This Article focuses on the privacy concerns that IoToys raises. Part II briefly outlines the evolution of IoToys while examining its devices' capacity to collect and retain data. Then, in reference to the legal framework chosen to protect children from online datafication twenty years ago, Part III discusses the American perception of children's privacy, focusing on COPPA. Through this analysis, this Part will show how key market players currently comply with COPPA regulation, and it will evaluate whether such compliance is relevant to IoToys's dangers and challenges. Part IV revisits COPPA, challenges it, and in calling for its recalibration, offers some practical solutions to IoToys's privacy threats. Thereafter, Part V normatively evaluates children's conception of privacy, argues that IoToys's monitoring practices could jeopardize the parent–child relationship, and calls for recalibrating children's privacy in the digital era. The final part summarizes the discussion and concludes that children's privacy matters today perhaps more than ever before and that the potential movement toward a ubiquitous surveillance era should not lead to its demise.

TABLE OF CONTENTS

I. INTRODUCTION

Children's toys are more communicative now than ever before. Implementing the advantages of what is commonly termed the *Internet of Things* (IoT),[1] many toy conglomerates have begun to produce and sell connected so-called smart toys, namely toys that can listen and actively respond to their users in real time. Being triggered, usually via a voice command, these toys will then send the message to a remote server, analyze it, and issue a timely response through the toy, as if it were talking to the child.[2]

Developments in this relatively new *Internet of Toys* (IoToys) market are advancing apace. At first, communicative toys were fairly limited in their communication abilities,[3] but now this expanding market offers various types of child-targeted toys and other devices that are both smart and connected to the internet.[4] Many are now equipped with microphones, speakers, cameras, and GPS trackers, along with other sensors designed to improve the toy's abilities, and ultimately the child's experience.[5]

IoToys devices sound almost like every child's dream. But while many benefits might accrue from their use, they may also quickly turn into nightmares.[6] Generally these toys, along with the cloud in which the gathered data is stored, could be hacked or accessed by third parties, thus exposing children to harmful content, and worse—endangering their personal safety and mental health.[7] More closely—and within the scope of this Article—children are also subjected to ubiquitous surveillance and datafication by toy conglomerates and their trusted partners, unauthorized third parties like hackers, and even their parents.[8] In other words, these seemingly harmless toys could

---

[1] The term Internet of Things may have been coined by Kevin Ashton as a part of a presentation for Proctor & Gamble. *See* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/articles/pdf?4986 [https://perma.cc/BY6Z-V2HM]. For more on the development of IoT, see Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things*,*"* 2017 U. ILL. L. REV. 415, 421–24 (2017).

[2] *See* discussion *infra* Part II.A.

[3] *See, e.g.*, Victoria Dawson, *The Epic Failure of Thomas Edison's Talking Doll*, SMITHSONIAN (June 1, 2015), http://www.smithsonianmag.com/smithsonian-institution/epic-failure-thomas-edisons-talking-doll-180955442 [https://perma.cc/VP3S-JEHB].

[4] *See* FUTURE OF PRIVACY F. & FAMILY ONLINE SAFETY INST., KIDS & THE CONNECTED HOME: PRIVACY IN THE AGE OF CONNECTED DOLLS, TALKING DINOSAURS, AND BATTLING ROBOTS 2 (Dec. 2016) [hereinafter KIDS & THE CONNECTED HOME], *available at* https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf [https://perma.cc/QV8P-U53U].

[5] *See infra* Part II.

[6] *See infra* note 48.

[7] *See infra* Part IV.B.4.

[8] This Article will use the term "parents" in reference to legal guardianship for minors in general. Subsequently, the use of the term "surveillance" will refer to various facets of monitoring and datafication of children's data within the Internet of Toys (IoToys). This type

potentially generate substantial harm, and perhaps worst of all, endanger children's right to privacy.

Potential datafication and misuse of children's data troubled policymakers long before the emergence of IoToys. Recognizing the potential dangers of the internet to children's privacy, American policymakers designed a framework known as the Children's Online Privacy Protection Act (COPPA) regulation, which applies to websites that target or knowingly collect personal information from children under age thirteen.[9] COPPA regulation was devised long before the invention of IoT,[10] but it remains the current regulatory framework governing IoToys. Do fundamental differences between websites and IoToys necessitate a different legal framework to protect children's privacy? Should policymakers recalibrate the current legal framework to adequately protect the privacy of children who have IoToys devices? And if so, how should it be done? Finally, what are the consequences for children's privacy of ubiquitous parental surveillance through IoToys—allegedly granted to safeguard children from online risks—and how might children's privacy be better framed and protected in this context?

This Article approaches these and related questions by analyzing the current legal framework fashioned twenty years ago to protect young children's privacy online and by examining—practically and normatively—how applicable it is to IoToys. Part II briefly introduces the evolution of IoToys and further examines the datafication of children within it. Part III scrutinizes children's right to privacy at the federal level as to whether COPPA regulation is applicable to IoToys. Then Part IV reevaluates children's privacy within the IoToys legal framework and proposes to recalibrate it in keeping with COPPA's requirements. Part V zooms out to discuss how children's privacy is affected by IoToys from the perspective of the parent–child relationship. It argues that children's privacy should not be viewed as protection just from third parties but also from their parents. Part VI summarizes the discussion and concludes that children's privacy is of profound importance, especially given a potential movement toward a ubiquitous surveillance era.

---

of surveillance could also refer to "dataveillance"—an abbreviation of data surveillance—described by Roger Clarke as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." Roger Clarke, *The Digital Persona and Its Application to Data Surveillance*, *in* 3 THE LIBRARY OF ESSAYS ON LAW AND PRIVACY: SECURITY AND PRIVACY 19, 25 (Joseph Savirimuthu ed., 2015).

[9] *See infra* Part III.A.

[10] *See infra* Part III.A.

II. THE INTERNET OF TOYS

Toys have existed almost as long as humanity itself. According to archaeologists, they date back at least four millennia.[11] While adults might occasionally play with them, traditional toys appeal mostly to children of various ages. But the meaning of *traditional* in the toy realm can change swiftly, considering technological innovations. Through the application of advanced learning capabilities and connection to the internet, many toys have become more interactive than ever before in human history[12] and most likely will continue to evolve for years to come.

Aside from their enjoyment and other potential educational and social benefits,[13] IoToys might also have a dark side. Along with IoToys devices' datamining capabilities, they could be exploited by various entities and eventually harm children and violate their legal rights.[14] For a better understanding of these concerns, Part II.A briefly tells the story of how toys became interactive from the first talking doll in 1890 to the latest technological developments of IoToys. The second section exposes and evaluates the potential dangers that IoToys raises in general and reviews the datamining practices of key market players in the IoToys industry to prepare the way for evaluating IoToys's implications for children's privacy.

A. *The Evolution of Connected Smart Toys*

In 1890, Thomas Edison introduced the first-ever talking doll to the world.[15] Edison inserted a miniature model of his phonograph into a doll's chest, which enabled it to recite a twenty-second rendition of a well-known rhyme.[16] Humanity, though, did not care for Edison's invention at that time, as the toy proved a commercial failure.[17] However, the importance of Edison's first-ever communicative toy lay mainly in its innovative thinking: it marked the potential birth of a new market, namely toys that could interact with children.

---

[11] *See* Amber Williams, *FYI: What Is the Oldest Toy in the World?*, POPULAR SCI. (Feb. 16, 2012), https://www.popsci.com/science/article/2012-01/what-oldest-toy-world [https://perma.cc/9SHH-8NWA].

[12] *See, e.g.*, Katie Lobosco, *Talking Barbie Is Too 'Creepy' for Some Parents*, CNN BUS. (Mar. 12, 2015), http://money.cnn.com/2015/03/11/news/companies/creepy-hello-barbie [https://perma.cc/2WX4-FW2X].

[13] *See infra* Part II.A.

[14] *See infra* Part II.A.

[15] Dawson, *supra* note 3. Edison's idea for commercializing his phonograph through dolls could be traced to a notebook entry in 1877. *See* James Vlahos, *Barbie Wants to Get to Know Your Child*, N.Y. TIMES (Sept. 16, 2015), https://www.nytimes.com/2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html [on file with *Ohio State Law Journal*].

[16] *See* Dawson, *supra* note 3.

[17] *Id.*

A market demand for interactive toys can be traced back to the early 1960s.[18] One of the key examples of this then-new market is pull-string dolls like Mattel's Chatty Cathy.[19] Only then did the market begin to thrive. Not long after Chatty Cathy's commercial success, Mattel introduced other communicative toys like See 'n Say.[20] Years later, other toy manufacturers followed suit by introducing communicative toys like Teddy Ruxpin and Furby.[21] Technology inspired life in toys, as they could now talk to children. At this stage, toys' abilities were still quite limited. Prior to the development of IoT, when ordinary objects became connected to the internet, toys' communication was still almost entirely one-sided. Even the most communicative toys had tightly limited storage capacity and learning capabilities, and they could not transfer data beyond their physical space, let alone analyze it and respond to their users.

With the development of IoT, and along with various devices targeted at children,[22] toys became more sophisticated or—stated differently—smarter. They began not only to repeat predefined phrases or well-known rhymes, but also to listen and respond. These *smart toys* interact with their users through an array of electronic features such as microphones, speakers, sensors, cameras, gyroscopes, and radio transmitters.[23] Besides smart toys, another form of new toys emerged, capable of connecting to an external network, mostly the internet, via a Wireless Fidelity (Wi-Fi) connection, cellular data networks, or Bluetooth.[24] These *connected toys* are designed to connect to the internet or

---

[18] *See, e.g.*, Olivia B. Waxman, *The 13 Most Influential Toys of All Time*, TIME (Oct. 29, 2014), http://time.com/3089384/influential-toys [https://perma.cc/P8PD-WQS9] (listing interactive toys that began being sold in the 1960s).

[19] *See* SHARON M. SCOTT, TOYS AND AMERICAN CULTURE: AN ENCYCLOPEDIA 60–61 (2010).

[20] *See* Allie Townsend, *See 'n Say*, TIME (Feb. 16, 2011), http://content.time.com/time/specials/packages/article/0288042049243_2048656_2049201,00.html [https://perma.cc/864R-D5TK].

[21] Teddy Ruxpin is a "talking" bear whose mouth and ears move while "reading" stories from an audio tape cassette. *See* Bridget Carey, *The Life, Death and Resurrection of Teddy Ruxpin*, CNET (Sept. 21, 2017), https://www.cnet.com/features/teddy-ruxpin-history-disney-atari-2017-return [https://perma.cc/5VEJ-T86W]. Furby is a toy first released in 1998 by Tiger Electronics Inc. that had the ability to "learn English." *Furby (1998)*, OFFICIAL FURBY WIKI, http://official-furby.wikia.com/wiki/Furby_(1998) [https://perma.cc/N23R-TS2Y].

[22] These devices include, inter alia, children's wearables, smartphones, and tablets. *See, e.g.*, Desire Athow, *Best Kids Tablets 2017: The Top Slates for Children*, TECHRADAR (Dec. 7, 2016), http://www.techradar.com/news/best-kids-tablets-2016-the-top-slates-for-children [https://perma.cc/CMH8-FS8E].

[23] *See* KIDS & THE CONNECTED HOME, *supra* note 4. It is notable that the use of the word "smart" to describe various types of devices and toys might be perceived as somewhat inaccurate to describe their true functions. Nevertheless, I generally use this term in this Article as it is often used by many to describe these devices and toys.

[24] *Id.* at 3–4.

other devices in order to receive and transmit data.[25] The combination of these two innovations led to the formation of *connected smart toys*, or more simply stated, IoToys. These toys could interact meaningfully with their users, hence they could be attractive to anyone, not just children. IoToys marked the birth of two-way communication toys.

Realizing a potential demand for IoToys devices, before long the market reacted. In 2015, Mattel collaborated with ToyTalk (later rebranded as PullString, Inc.) to introduce a Barbie doll that "actually listen[s] and talk[s] back."[26] Using speech recognition, Hello Barbie connects to the internet via Wi-Fi, and by the press of a buckle button on its belt, Hello Barbie turns its microphone on and begins recording.[27] The data is then sent from the doll to a cloud-based service of ToyTalk, and following analysis, a response is streamed back to the user through the doll's speaker.[28]

Hello Barbie clearly marked the beginning of a thriving new market.[29] To name a few examples, following Hello Barbie, Mattel introduced the Hello Barbie Dreamhouse (hereinafter The Dreamhouse), a smart connected home for Barbie dolls;[30] Fisher-Price, a subsidiary of Mattel, introduced a Wi-Fi-connected smart toy bear that "talks, listens, and 'remembers' what your child says and even responds when spoken to";[31] CogniToys introduced various

---

[25] Smart toys and connected toys are not necessarily synonymous. The fact that a toy is smart does not mean it is connected, nor the other way around. Smart toys could be offline and connected toys might not be equipped with technological capabilities to elevate them to the level of being categorized as "smart." For more on smart and connected toys, see *id.* at 2.

[26] Lobosco, *supra* note 12.

[27] *See* Iain Thomson, *Hello Barbie: Hang on, This Wi-Fi Doll Records Your Child's Voice?*, THE REGISTER (Feb. 19, 2015), http://www.theregister.co.uk/2015/02/19/hello_barbie [https://perma.cc/4HS4-WX4D].

[28] *See* Lobosco, *supra* note 12; Joseph Steinberg, *This New Toy Records Your Children's Private Moments -- Buyer Beware*, FORBES (Mar. 20, 2015), http://www.forbes.com/sites/josephsteinberg/2015/03/20/this-new-toy-records-your-childrens-private-moments-buyer-beware/#2d7698951ab9 [https://perma.cc/ZK9E-UJYT].

[29] It seems that it will not take long before market players expand their variety of IoToys devices and new companies will join this growing market. Google, for instance, has filed a patent request back in 2015 for a teddy bear outfitted with sensors and cameras. *See* Hope King, *Google Files Patent for Creepy Teddy Bear*, CNN (May 22, 2015), http://money.cnn.com/2015/05/22/technology/google-doll-toy-connected-device-patent [https://perma.cc/PG24-ZGGL]; Press Release, Juniper Res., Smart Toy Revenues to Hit $2.8BN This Year, Driven by Black Friday & Christmas Holiday Sales (Nov. 9, 2015), https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-$2-8bn-this-year [https://perma.cc/8CK5-LJUT].

[30] *See Barbie® Hello Dreamhouse™*, BARBIE, https://barbie.mattel.com/en-us/about/hello-dreamhouse.html [https://perma.cc/U2H5-G8HQ].

[31] Duncan Riley, *There's a Hacker in There: Security Vulnerabilities Found in Fisher Price, hereO GPS Kids Toys*, SILICON ANGLE (Feb. 2, 2016), https://siliconangle.com/2016/02/02/theres-a-hacker-in-there-security-vulnerabilities-found-in-fisher-price-hereo-gps-kids-toys/ [https://perma.cc/4QZN-SEB7]. *See generally Smart Toy® Bear*, FISHER-PRICE, http://fisherprice.mattel.com/shop/Product2_10151_10101_18442_-1 [https://perma.cc/

cloud-connected toy dinosaurs that listen to children's questions and answer according to their age;[32] and Genesis, a company incorporated under the laws of Hong Kong, introduced My Friend Cayla (hereinafter Cayla), a doll that could talk and interact with users, play games, share photos, and read stories.[33] This market appears to be growing continuously.[34]

The children's IoT market has recently expanded beyond toys. This expansion was first proclaimed early in 2017, when Mattel, under its "Nabi" brand, announced its plan to manufacture a smart Wi-Fi-connected speaker for children.[35] This device, named Aristotle, was supposed to be equipped with a microphone, LEDs, and a camera,[36] and it was designed to act like a computerized personal assistant akin to Amazon Echo or Google Home,[37]

4CVZ-3QGJ] (describing the current range of toys).

[32] *See Part Toy. Part Pal. All Awesome.*, COGNITOYS, https://cognitoys.com/pages/about [https://perma.cc/W8ZX-TKRV].

[33] Upon downloading the App, users can ask Cayla questions which will be answered by "Internet sources" like Google Search, Wikipedia, and Weather Underground. *See Privacy Policy*, MY FRIEND CAYLA, https://www.myfriendcayla.com/privacy-policy (last updated Feb. 23, 2015) [https://perma.cc/CNL8-A4NQ]; *This Is Cayla*, MY FRIEND CAYLA, https://www.myfriendcayla.com/meet-cayla-c8hw [https://perma.cc/DLY2-E6WG].

[34] For a prediction on the future of IoToys, see, for example, *Global Smart Toys Market Will Reach USD 5,410.00 Million by 2024: Zion Market Research*, GLOBENEWSWIRE (Sept. 5, 2018), https://globenewswire.com/news-release/2018/09/05/1565750/0/en/Global-Smart-Toys-Market-Will-Reach-USD-5-410-00-Million-By-2024-Zion-Market-Research.html [https://perma.cc/V9CF-436T].

[35] *See* Rob Verger, *Mattel Touts Aristotle, an Amazon Echo-Style Device for Children*, FOX NEWS (Jan. 4, 2017), http://www.foxnews.com/tech/2017/01/04/mattel-touts-aristotle-amazon-echo-style-device-for-children.html [https://perma.cc/4SH5-VJEN].

[36] *See id.*

[37] Computerized personal assistants (also known as intelligent personal assistants) are software agents that can perform tasks or services for an individual, usually based on user input, location awareness, and the ability to access information from a variety of online sources. There are various types of computerized personal assistants, e.g., Apple's Siri and Microsoft's Cortana. Google had even embedded such technology in 2014, under a pre-installed ability in Google's Chrome browser that passively listened for the words "OK, Google" to launch a voice-activated search function. *See* Tony Bradley, *'OK Google' Feature Removed from Chrome Browser*, FORBES (Oct. 17, 2015), http://www.forbes.com/sites/tonybradley/2015/10/17/ok-google-feature-removed-from-chrome-browser/#16d299a44e27 [https://perma.cc/Y9TZ-9JU3]; *Top 22 Intelligent Personal Assistants or Automated Personal Assistants*, PAT RES., http://www.predictiveanalyticstoday.com/top-intelligent-personal-assistants-automated-personal-assistants/#content-anchor [https://perma.cc/DQ9Z-FW3M]. More specifically, Amazon Echo is "a hands-free speaker you control with your voice." *Amazon Echo*, AMAZON, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E [https://perma.cc/C6XL-KZZQ]. It "connects to the Alexa Voice Service to play music, . . . provide information, news, sports scores, weather, and more—instantly. . . . When you want to use Echo, just say the wake word 'Alexa' and Echo responds instantly." *Id.* Google Home is a voice-activated speaker powered by the Google Assistant. "Ask [it] questions. Tell it to do things. It's your own Google, always ready to help." *Google Home Devices*, GOOGLE HOME HELP,

programmed for children's purposes.[38] As for now, Mattel decided that Aristotle is not fit for release, and its future is still uncertain.[39] Mattel, however, currently still plans to release the Hello Barbie Hologram (hereinafter The Hologram): a small box with an animated projection of Barbie that responds to voice commands.[40] Closely akin to computerized personal assistants like Amazon Echo or Google Home, the Hologram uses a wake phrase ("Hello Barbie"), so unlike Hello Barbie, this device operates in an "always on" mode: for the device to begin functioning, it must constantly listen for the wake phrase.[41] Respectively, Amazon had already entered this market recently, introducing the Echo Dot "Kids Edition"—a standard Echo Dot with "parental controls, kid-friendly content, and an optimized experience for kids."[42] All in all, as could be drawn from these innovative projections of new devices, IoT will most likely play a substantive role in child-targeted devices in the foreseeable future.

IoToys presents children with interactive playing. Beyond the toys' fun, they could carry educational and social benefits for children: opportunities to learn, pick up, and improve communication skills; retain interest in playing despite children's short attention spans; encourage active play and toy interaction, which might be preferable to passive screen time; foster collaborative play with other children; identify learning difficulties or medical problems; and be economically efficient for parents because their software could be updated.[43] On the other hand, IoToys devices have been criticized for

---

https://support.google.com/googlehome/answer/7029281?hl=en [https://perma.cc/5WFY-NYKU].

[38] *See* Verger, *supra* note 35. Another potential smart assistant for children is "Smarty," which, according to its manufacturer, is equivalent to an Amazon Echo for children. *See* Zoë 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 [https://perma.cc/DEH4-8EA5].

[39] *See* Eric Franklin, *Mattel Won't Release Its Aristotle Child Monitor After All*, CNET (Oct. 5, 2017), https://www.cnet.com/news/mattel-just-cancelled-its-aristotle-child-monitor [https://perma.cc/Q2DP-MM49].

[40] *See* Tim Moynihan, *So, Barbie's a Hologram Now. Oh, and She Responds to Your Voice*, WIRED (Feb. 17, 2017), https://www.wired.com/2017/02/hello-barbie-hologram-matell [https://perma.cc/L3GC-8Z9X].

[41] An "always on" mode refers to devices where there is no need to physically push a button to turn them on, but rather they are activated by a voice command or through the device app. Using speech recognition, users simply need to say a trigger phrase to activate them. Examples include Amazon Echo and Google Home, both activated by a trigger phrase such as "Alexa" or "OK Google" respectively, and once activated record the voice command of their user. *See* sources cited *supra* note 37.

[42] Dan Seifert, *Amazon's New Echo Dot Kids Edition Comes with a Colorful Case and Parental Controls*, THE VERGE (Apr. 25, 2018), https://www.theverge.com/2018/4/25/17276164/amazon-echo-dot-kids-edition-freetime-price-announcement-features-specs [https://perma.cc/73CA-6DAX].

[43] *See* Stéphane Chaudron et al., *Kaleidoscope on the Internet of Toys: Safety, Security, Privacy and Societal Insights*, JRC TECHNICAL REP. 9 (2017), http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf [https://perma.cc/6CV

their potential educational, social, and psychological drawbacks.[44] To name a few: providing poor quality of play; potentially harming children's development, impeding child–parent interaction;[45] obstructing children's well-being and healthy development, which require real relationships and conversations;[46] and posing a risk to health from electromagnetic radiation (EMR).[47]

IoToys devices' potential drawbacks do not stop there. They might subject children to various risks, for example, exposure to harmful content.[48] There is even the danger of mental and bodily harm by predators, some of whom could have access toys and use them to listen to, watch, track, and even directly contact children.[49] Along with these important challenges, these IoToys devices further raise human rights concerns. Potentially, they can subject children to ubiquitous surveillance and datafication, which could profoundly impact their right to privacy.[50] To normatively assess the privacy challenges—which is the core

---

A-B3FY]; *5 Benefits of Tech Toys for Children,* ROBO WUNDERKIND (June 23, 2017), http://yuriy-levin.squarespace.com/blog/benefits-tech-toys-kids [https://perma.cc/Q599-U3A8].

[44] *See* Kate Cox, *Privacy Advocates Raise Concerns About Mattel's Always-On 'Aristotle' Baby Monitor*, CONSUMERIST (May 10, 2017), https://consumerist.com/2017/05/10/privacy-advocates-raise-concerns-about-mattels-always-on-aristotle-baby-monitor [https://perma.cc/VP3S-JEHB].

[45] Digital caretaking could negatively affect children's development as it lacks necessary physical bonding. *See id.*

[46] *See, e.g.*, Richard Chirgwin, *Mattel's Parenting Takeover Continues with Alexa-Like Dystopia*, THE REGISTER (Jan. 4, 2017), https://www.theregister.co.uk/2017/01/04/mattels_parenting_takeover_continues_with_alexalike_dystopia [https://perma.cc/NXP5-7GW3].

[47] *See* Chaudron et al., *supra* note 43, at 9.

[48] As these toys rely on remotely stored data, they could be subjected to harmful content as information might become vulnerable and could be changed by a malicious entity which gained access to the toy or simply due to bad or error in programing. See, for instance, how a misunderstanding led Amazon Echo to spout porn search terms to a toddler. *Amazon Alexa Gone Wild*, YOUTUBE (Dec. 29, 2016), https://www.youtube.com/watch?v=r5p0gqCIEa8 [https://perma.cc/SE3G-M5ZU]. See also how a specialist team hacked Cayla to quote Hannibal Lecter and lines from *50 Shades of Grey*. *See* David Moye, *Talking Doll Cayla Hacked to Spew Filthy Things*, HUFFPOST (Feb. 9, 2015), http://www.huffingtonpost.com/2015/02/09/my-friend-cayla-hacked_n_6647046.html [https://perma.cc/78HN-89F6].

[49] When children assume that it is the toy that is "talking" to them, predators might be able to persuade them to convey sensitive information. These predators could obtain information from children like where they live and, perhaps even worse, convince them to act on their behalf. *See* Abby Haglage, *Hackable 'Hello Barbie' the Worst Toy of the Year (and Maybe Ever)*, DAILY BEAST (Dec. 10, 2015), http://www.thedailybeast.com/hackable-hello-barbie-the-worst-toy-of-the-year-and-maybe-ever [https://perma.cc/85E4-AGQW]. For a typology of risks to children online, see ORG. FOR ECON. CO-OPERATION & DEV. (OECD), THE PROTECTION OF CHILDREN ONLINE - RECOMMENDATION OF THE OECD COUNCIL REPORT ON RISKS FACED BY CHILDREN ONLINE AND POLICIES TO PROTECT THEM 24–39 (2012), https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf [https://perma.cc/33T7-R645].

[50] For more on children's right to privacy, see *infra* Part III.A.

purpose of this Article—the next section briefly surveys the proclaimed datamining practices of key market players in the IoToys realm.

B. *Surveillance and Datafication of Children in IoToys*

While toys have evolved to become smarter and connected, the various IoToys devices may evince wide differences.[51] Some are smarter than others. Some are equipped with more technological tools that enhance their capabilities; others are simply more sophisticated, for example, by being equipped with a microphone, while others have cameras and other sensors. Some, like Hello Barbie, require their users to turn them on manually,[52] while others, like the Dreamhouse and the Hologram, operate in an "always on" mode, namely by constantly operating as they await their wake phrase.[53] Yet their different characteristics notwithstanding, the core functions of IoToys devices are fairly similar: upon activation, each toy acquires data from its user, sends it to a remote server where it is analyzed, and transmits a response through the toy's speaker. Datamining is essentially at the core of their functioning.

Take, for example, Mattel, which manufactures several types of IoToys and connected smart devices such as Hello Barbie (doll and hologram) and the Dreamhouse. The speech processing services for Hello Barbie and the Dreamhouse (hereinafter Barbie Products) are currently operated by ToyTalk.[54] Barbie Products capture recordings upon users' interaction with them, whether by pressing the "talk" button or saying the wake phrase.[55] Other products, like Cayla, also capture their users' recording, usually after a wake phrase.[56] Fisher-Price's Smart Toy bear collects a parent's email address and login password; child's first name, birthdate, and gender; toy name and identifier; Wi-Fi password; and mobile device information.[57] Essentially, most of these IoToys devices capture audio recordings and collect some forms of data.

The information mined through these toys is then stored, usually in the cloud, for various purposes.[58] Obviously, data can be highly valuable for various

---

[51] For an analysis of how IoToys devices operate, see Junia Valente & Alvaro A. Cardenas, *Security & Privacy in Smart Toys*, IOTS&P'17, 19 (2017).

[52] Thomson, *supra* note 27.

[53] *See* Moynihan, *supra* note 40.

[54] *See Privacy Policy*, TOYTALK, https://www.toytalk.com/hellobarbie/privacy [https://perma.cc/D8V5-UBQA] [hereinafter TOYTALK, *Privacy*].

[55] *See id.* ("When children or other users talk with Hello Barbie by pressing and holding the 'Talk' button, interact with Barbie Hello Dreamhouse after saying the Gate Phrase, or record their voice to customize the sounds in a room, we may capture voice recordings.").

[56] *Privacy Policy*, *supra* note 33; *This Is Cayla*, *supra* note 33.

[57] MINORITY STAFF OF S. COMM. ON COMMERCE, SCI., & TRANSP., 114TH CONG., REP. ON CHILDREN'S CONNECTED TOYS: DATA SECURITY AND PRIVACY CONCERNS 12 (Comm. Print 2016) [hereinafter CHILDREN'S CONNECTED TOYS]. Images and audio, however, are currently only stored locally on the bear. *Id.*

[58] ToyTalk and Genesis both mention that they store voice recordings in the cloud. ToyTalk announced that they may "use, store, process, convert, transcribe, analyze or review

interested parties for a variety of business purposes, much like any data gathered online.[59] Data can potentially be commercialized and shared with other interested parties.[60] From a functional aspect, data could be valuable for the toy's improvement. As some toy manufacturers and online service providers (OSPs) posit, the entertainment experience from the toy is based to some extent on the audio recordings sent from it, which are then analyzed and stored.[61] Improving the functioning of the speech-processing services is essential, as is the development, testing, and improvement of speech-recognition technology and artificial-intelligence algorithms;[62] likewise the development of acoustic and language models.[63] It might also be necessary for other research, development, and data analysis purposes.[64] Finally, in the sense of innovation, companies might need the data to ameliorate services, functionality, and the development of other toys and devices in the IoT market.

To recap briefly, while it is difficult to assess how and to what extent the collected data is used, and by whom, these companies evidently are able to capture various types of data. Toys with microphones could allow listening to and recording any conversations taking place in relatively close proximity to the toys. Toys equipped with sensors could give third parties access to data in real-time from these sensors. Toys with GPS trackers let third parties know where the toys are currently located and where they have been since they were first

---

voice recordings." *See, e.g.*, TOYTALK, *Privacy*, *supra* note 54. As for the Hologram, however, Mattel announced that it does not save the recordings in its servers. *See* Moynihan, *supra* note 40.

[59] *See, e.g.*, Grace Chung & Sara M. Grimes, *Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games*, 30 CAN. J. COMM. 527, 533 (2005).

[60] Genesis, for instance, mentions that upon consent, they are entitled to collect, process, maintain, and transfer personal information in and to the United States and other applicable territories in which their privacy laws are not as comprehensive as or equivalent to those in the country where the data subject resides or is a national. They also share information with "trusted partners" and other entities in the "family of companies controlled by Genesis" for internal reasons, primarily for business and operational purposes. *See Privacy Policy*, *supra* note 33. ToyTalk shares captured data with third parties under exception listed in the privacy policy. Interestingly, however, ToyTalk claims that they will not share voice recordings with Mattel, rather only anonymized information that does not count as personal information. *See* TOYTALK, *Privacy*, *supra* note 54; *Hello Barbie and Hello Dreamhouse Privacy FAQ*, TOYTALK, https://toytalk.com/hellobarbie/privacyfaq [https://perma.cc/57MY-4ZAA] [hereinafter TOYTALK, *FAQ*].

[61] ToyTalk claims that they use audio recordings to create the entertainment experience. According to Martin Reddy, a chief technical officer at ToyTalk, analyzing recordings enables ToyTalk to boost the accuracy of what Hello Barbie hears by about 15%. *See* Mark Harris, *Virtual Assistants such as Amazon's Echo Break US Child Privacy Law, Experts Say*, THE GUARDIAN (May 26, 2016), https://www.theguardian.com/technology2016/may/26/amazon-echo-virtual-assistant-child-privacy-law [https://perma.cc/EKT5-DN93]. It should also be further noted that ToyTalk archives users' play sessions. *See* TOYTALK, *FAQ*, *supra* note 60.

[62] *See* TOYTALK, *Privacy*, *supra* note 54; *Privacy Policy*, *supra* note 33.

[63] *See* TOYTALK, *Privacy*, *supra* note 54.

[64] *Id.*

configured. And finally, toys equipped with cameras could enable third parties to see what the toys are currently seeing. These companies can then store the data for indefinite periods, use it for their own purposes, and share it with interested parties.

While children's datafication in IoToys might be integral for the toys' existence and development, it also raises substantial privacy concerns. How can we properly safeguard the data aggregated through IoToys from authorized and unauthorized entities that have gained access to the data? Does the current American legal framework[65]—originally crafted to protect children online—apply to IoToys? And does it adequately protect their right to privacy? To answer these questions, the next Part revisits and evaluates children's right to privacy in light of IoToys.

III. REGULATING PRIVACY WITHIN THE INTERNET OF TOYS

It is generally uncontested that children require special care and assistance.[66] As a cohort, they are less equipped with the skills and cognitive ability to comprehend some risks and concerns as adults do, let alone the depth and complexity of human rights and liberties.[67] They might lack the requisite "maturity, [ability,] knowledge, or experience to protect themselves,"[68] and they could be more trusting than adults.[69] They might value their immediate needs more than their long-term interests,[70] not understand the true nature or appropriate use of the collected information,[71] and value privacy differently from their parents.[72] In other words, while accounting for potential age

---

[65] This Article focuses on the federal level, but it is also important to note that state legislators also enact privacy laws which could be applicable on IoToys as well. For more on states' privacy legislation, see, for example, DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 145–56 (Int'l Ass'n of Privacy Professionals ed., 2015).

[66] Many consider childhood to be entitled to special care and assistance. On the global level, see G.A. Res. 44/25, United Nations Convention on the Rights of the Child (Nov. 20, 1989). For a detailed report on online risks to children, see INTERNET SAFETY TECH. TASK FORCE TO THE MULTI-STATE WORKING GRP. ON SOCIAL NETWORKING OF STATE ATTORNEYS GEN. OF THE U.S., ENHANCING CHILD SAFETY AND ONLINE TECHNOLOGIES (John Palfrey et al. eds., 2008).

[67] *See* Nicholas W. Allard, *Privacy On-Line: Washington Report*, 20 HASTINGS COMM. & ENT. L.J. 511, 529 (1998).

[68] Danielle J. Garber, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 132 (2001).

[69] Dorothy A. Hertzel, Note, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online,* 52 FED. COMM. L.J. 429, 434 (2000).

[70] Emmanuelle Bartoli, *Children's Data Protection vs Marketing Companies*, 23 INT'L REV. L. COMPUTERS & TECH. 35, 37 (2009).

[71] *See* Jerry S. Birenz, *Caching World Wide Web Sites*, 16 COMM. LAW. 13, 13 (1998); Hertzel, *supra* note 69, at 434.

[72] *See* Emily Nussbaum, *My So-Called Blog*, N.Y. TIMES (Jan. 11, 2004), https://www.nytimes.com/2004/01/11/magazine/my-so-called-blog.html [on file with *Ohio State Law Journal*]. For more on children's perception of privacy, see *infra* Part V.B.

differences, children often need guidance on various aspects of their lives, including how to properly protect their privacy.

A. *Children's Right to Privacy*

There are many different views on what privacy means and how best to protect it.[73] The modern concept of privacy is generally attributed to the famous law review article by attorneys Samuel Warren and future Supreme Court Justice Louis Brandeis, published in the same year that Edison introduced the first-ever talking doll, which articulated the right to privacy as the "right to be let alone."[74] Since then, privacy scholars have articulated the right to privacy diversely. Key examples include the classic "control theory," which conceptualizes privacy as the right to control information about oneself;[75] "limited access theory," which posits that privacy is related to our concern about our accessibility to others;[76] and a conceptual framework of privacy as "contextual integrity," which links the protection of personal information to the norms of specific contexts.[77] Without belittling the importance of this scholarly debate, privacy in the context of this Article is scrutinized from the viewpoint of children, who require special protection from the harm that the internet entails, under the American approach known as "sectoral privacy."[78]

American policymakers chose this sectoral approach to privacy, seeking to provide legal safeguards that would presumably improve children's safety

---

[73] For a taxonomy of privacy, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 484–91 (2006).

[74] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[75] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1968) ("[T]he claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.").

[76] *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980). *See generally* ANITA ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988) (introducing a range of privacy and privacy-related problems confronting American women).

[77] *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010) (detailing privacy considerations relevant in the context of rapidly developing technology).

[78] Sectoral privacy can be loosely defined as regulation that is directed to specific industries or a cohort (like children) and depends also on types of information. Generally, data privacy protection in the American legal system is protected under this sectorial approach, i.e., by specific targeted rules. Beyond the data protection of young children through COPPA, see generally Fair Credit Reporting Act, 15 U.S.C. §§ 1681a–1681x (2012) and Gramm–Leach–Bliley Act, 15 U.S.C. §§ 6801–6809 (2012) (regulating financial information); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, 110 Stat. 1936 (1996) (regulating healthcare and medical information); Video Privacy Protection Act, Pub. L. No. 100–618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710–2712 (2012)) (protecting individuals' videotape rental information); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003).

online and reasonably secure their privacy.[79] In 1998, under this perceived need to protect children's privacy online,[80] Congress enacted the Children's Online Privacy Protection Act (COPPA).[81] To supplement COPPA, the Federal Trade Commission (FTC) issued a rule, last updated in 2013, which is commonly referred to as the "COPPA Rule."[82] Both forms of regulation (hereinafter COPPA regulation) were crafted to prohibit unfair or deceptive acts or practices in connection with personal information from and about children on the internet; it is enforced by the FTC.[83]

---

[79] *See* The Child Online Protection Act, Pub. L. No. 105–277, 112 Stat. 2681–736 (1998). Information privacy was defined by the Clinton Administration's Information Infrastructure Task Force as "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used." INFO. INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION 1 (1995). The conventional concept of information privacy refers to protecting a right to control one's personal data. For further reading on information privacy, see generally Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000) (exploring the divergence in internet privacy approach and substance between Europe and the United States).

[80] It is worth mentioning that Congress also sought to regulate the exposure of children to inappropriate materials online by enacting the Child Online Protection Act (COPA), but it eventually failed to pass constitutional muster as it placed an "impermissible burden" on speech. *See* The Child Online Protection Act, Pub. L. No. 105–277, 112 Stat. 2681–736 (1998); ACLU v. Reno, 217 F.3d 162, 166–69 (3d Cir. 2000).

[81] It should be stressed that COPPA was passed following dozens of rejected privacy bills. In addition, prior to COPPA, Congress enacted the Family Educational Rights and Privacy Act (FERPA) in 1974, which also regulates children's informational privacy and family privacy. FERPA, however, applies only on the release of educational records to unauthorized persons by educational institutions. *See* The Family Educational Rights and Privacy Act (FERPA), Pub. L. No. 93–380 (1974) (codified at 20 U.S.C. § 1232g (2012)); *Family Educational Rights and Privacy Act (FERPA)*, 3 U.S. DEP'T EDU., http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html [https://perma.cc/XN5A-K4J2]; *see also* Kathryn C. Montgomery & Jeff Chester, *Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework*, 1 EUR. DATA PROT. L. REV. 277, 279–80 (2015) (discussing the key factors that shaped COPPA and explaining its legacy for the digital children's marketplace and U.S. regulation).

[82] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2012)) [hereinafter COPPA Rule]. COPPA Rule has been effective since April 2000. For the latest update, see 78 Fed. Reg. 3972 (Jan. 17, 2013).

[83] 15 U.S.C. §§ 6501–6505 (2012); COPPA Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2012)); Garber, *supra* note 69, at 153.

> An 'unfair or deceptive' act or practice is a material 'representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment' or a practice that 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'

Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014) (internal citations omitted). Substantial injury, in this

COPPA regulation applies to OSPs that target children under the age of thirteen[84] or knowingly collect personal information from them.[85] An OSP is any person operating an online service, including websites, "who collects or maintains personal information from or about the users of, or visitors to," such online services.[86] It also includes any person "on whose behalf such information is collected or maintained, where such a website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce."[87]

As a form of market self-regulation—commonly termed *privacy self-management*,[88] COPPA incorporates five essential Fair Information Practice Principles (FIPPs):[89] (1) Notice, (2) Choice, (3) Access, (4) Security, and (5) Enforcement.[90] Websites that fall under COPPA regulation must include a

---

instance, could apply on both financial harms and unwarranted health and safety risks. *See* Complaint for Injunctive and Other Equitable Relief at ¶ 12, FTC v. Information Search, Inc., No. 06CV01099, 2006 WL 1882455 (D. Md. Mar. 9, 2007) ("The invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers."); 15 U.S.C. § 45 (2012) ("Unfair methods of competition unlawful").

[84] While arguably, choosing the age of thirteen is somewhat arbitrary, it is beyond this Article's scope to examine this controversy. For such criticism, see, for example, Bartoli, *supra* note 70, at 38.

[85] *Id.*

> *Personal information* means individually identifiable information about an individual collected online, including: (1) A first and last name; (2) A home or other physical address including street name and name of a city or town; (3) Online contact information as defined in this section; (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section; (5) A telephone number; (6) A Social Security number; (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. . . . ; (8) A photograph, video, or audio file where such file contains a child's image or voice; (9) Geolocation information sufficient to identify street name and name of a city or town; or (10) Information concerning the child or [parent] that the operator collects online from the child and combines with an identifier described in this definition.

16 C.F.R. § 312.2 (2012); *see* 15 U.S.C. § 6501(8) (2012).

[86] 15 U.S.C. § 6501(2) (2012).

[87] *Id.*

[88] Privacy self-management is an approach to privacy regulation whereas the law provides people with a set of rights, e.g., primarily rights to notice, access, and consent regarding the collection, use, and disclosure of personal data, to enable them to make decisions about how to manage their data. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

[89] More generally, Fair Information Practice Principles (FIPPs) includes notice, access, choice, accuracy, data minimization, security, and accountability. *See* Shackelford et al., *supra* note 1, at 441.

[90] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS i, 4 (May 2000), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-

notice containing what information is collected, how it is used, and its information disclosure practices.[91] OSPs must "obtain *verifiable parental consent* for the collection, use, or disclosure of such personal information from children."[92] The parent of a child who supplies personal information must have the right *to obtain* "*a description* of the specific types of personal information collected from the child by that operator" and have "the opportunity at any time *to refuse to permit the operator's further use or maintenance . . . or future online collection,* of personal information from that child."[93] The operator must also provide reasonable means, in the given circumstances, for "the parent *to obtain any personal information collected from that child*."[94] COPPA further prohibits "conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity."[95] In terms of security, COPPA regulation requires OSPs to "*establish and maintain reasonable procedures* to protect the confidentiality, security, and integrity of personal information collected from children."[96]

To enforce COPPA regulation, the FTC has the authority to create rules and police unfair and deceptive trade practices, which include private companies' privacy policies.[97] Consequently, it can issue fines and seek preliminary or permanent injunctive remedies for those who do not comply with COPPA regulation.[98] While to date most cases have resulted in settlement agreements,[99]

---

practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [https://perma.cc/A5SV-YZ2A]; Garber, *supra* note 69, at 153.

[91] 15 U.S.C. § 6502(b)(1)(A)(i) (2012).

[92] *Id.* § 6502(b)(1)(A)(ii) (emphasis added).

[93] *Id.* § 6502(b)(1)(B) (emphasis added).

[94] *Id.* (emphasis added).

[95] *Id.* § 6502(b)(1)(C).

[96] 16 C.F.R. § 312.3(e) (2012) (emphasis added).

[97] 15 U.S.C. §§ 6501–6506 (2012). The FTC authority stems from both The Federal Trade Commission Act of 1914 (FTC Act), ch. 311, §5, 38 Stat. 719 (codified at 15 U.S.C. §§ 45(a), 6505(a) (2012)) and COPPA. It has the authority to promulgate and update rules under the Administrative Procedure Act (APA) (codified at 15 U.S.C. § 6502(b) (2012)). *See* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 811 (2011); Solove & Hartzog, *supra* note 83, at 588.

[98] 15 U.S.C. §§ 45(l)–(m), 53(b) (2012). In 2016, a group of toy and children's entertainment conglomerates were fined by the FTC in the amount of $835,000 for letting advertisers illegally track kids online. Shaun Nichols, *Viacom, Mattel and Pals Busted for Stalking Kids with Creepy Web Ads*, THE REGISTER (Sept. 14, 2016), http://www.theregister.co.uk/2016/09/14/viacom_mattel_busted_for_tracking_kids [https://perma.cc/37C9-XHKY]. Violating COPPA requirements could currently lead to fines up to $40,000 per violation. *See* Adjustment of Civil Monetary Penalty Amounts, 81 Fed. Reg. 42476 (June 30, 2016).

[99] *See* Solove & Hartzog, *supra* note 83, at 585. The FTC reported that concerning data security, they "entered into approximately 60 settlements related to companies' failure to protect consumers' personal information." *See* Letter from Maureen K. Ohlhausen, Acting

the FTC reported that from 2000 to 2016 it "brought over 20 COPPA cases and collected millions of dollars in civil penalties."[100]

COPPA has received much scholarly attention since its inception,[101] but it now extends far beyond regulation for the internet. Being online in 2019 means something different than what it meant back in the late 1990s when COPPA was enacted. Naturally, Congress could not have foreseen the technological developments that might pose new threats to children like that of IoT. Despite these developments, COPPA regulation still governs the datafication of children online. Does COPPA apply to IoToys and other devices within the IoToys market? Are the legal safeguards to protect children's privacy under COPPA—initially set twenty years ago—still relevant to regulate IoToys? How should policymakers balance the potential benefits of this innovative technology with the dangers they entail for children?

B. *Applicability of the Legal Framework*

Although crafted long before the emergence of IoToys, COPPA regulation undoubtedly applies on them. These toys generally target children, and most—if not all—should be labeled as targeting children aged under thirteen. Even if the prime audience for some of these toys is arguably older than thirteen, COPPA will still apply when those OSPs knowingly collect personal information from younger children.[102] This second category encompasses gathering any personal information from a child, including the following: (1) "Requesting, prompting, or encouraging a child to submit personal information online ; (2) Enabling a child to make personal information publicly available in identifiable form. . . . or (3) Passive tracking of a child online."[103]

Chair, Fed. Trade Comm'n, to Senator Mark R. Warner (June 22, 2017) [hereinafter Letter to Senator Warner], *available at* https://www.scribd.com/document/352278126/2017-06-21-Response-to-Senator-Warner-Letter [https://perma.cc/GH58-HM2A].

[100] *See* FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE (Jan. 2017), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2016#children [https://perma.cc/HYX5-PB9H].

[101] While many articles that relate to COPPA are further cited within this Article, here are few examples of such scholarly work: Garber, *supra* note 69 (discussing the need for privacy with respect to the increase in technology use by children); Solove & Hartzog, *supra* note 83 (examining the FTC's privacy law jurisprudence); Joseph A. Zavaletta, *COPPA, Kids, Cookies & Chat Rooms: We're from the Government and We're Here to Protect Your Children*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 249 (2000–2001) (examining the evolution of the need for privacy online); Joshua Warmund, Note, *Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 189 (2000) (analyzing the parental consent measures in COPPA).

[102] *See* 16 C.F.R. § 312.2(1)–(2) (2012).

[103] *Id.* § 312.2(1)–(3). Note, however, that an OSP will not be considered to have collected personal information under the COPPA rule "if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also delete such information from its records." *Id.* § 312.2(2).

Children's data in IoToys easily fall within these definitions. The mere use of IoToys devices that children can talk to should be deemed a way of encouraging the child to submit personal information.[104] To clarify the applicability of COPPA to IoToys, the FTC recently stated clearly that "connected toys or other Internet of Things devices" will be deemed a website or online service for COPPA regulation.[105]

While the IoToys market is rapidly expanding, not all toys raise similar concerns. Smart toys that are not connected to the internet naturally do not raise COPPA-related concerns.[106] Connected toys, while potentially able to trigger COPPA regulation, pose no risks to children's privacy as long as their ability to collect, retain, and transmit data is relatively low to non-existent, and as long as connecting to them, lawfully or not, cannot generate sensitive information.[107] It might be presumptuous to assume that all IoToys devices trigger COPPA by default, but at least the majority of this market will easily fall under one of COPPA's categories. For example, audio recordings containing a child's voice or imagery, if collected by an OSP, would suffice to be deemed personal information under COPPA.[108] In addition, when a device enables recording and transmitting data, it could potentially capture personal data such as the name, home address, online contact information, and even social security numbers of children, and thus might also trigger COPPA.[109]

Having established that COPPA generally applies to IoToys, the next question is whether OSPs comply with their legal obligations. As noted, COPPA regulation necessitates OSPs to meet the following five requirements: "(1) notice; (2) [verifiable] parental consent prior to the collection, use, and/or disclosure of personal information from a child; (3) a right of parental review of such information; (4) proportionality; and (5) reasonable security policies.[110] To enjoy safe haven from enforcement action under COPPA regulation, companies could also follow self-regulatory guidelines pre-approved by the FTC.[111] As for

---

[104] *See id.* § 6502(b)(1)(C)–(D).

[105] *See Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FED. TRADE COMM'N (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [https://perma.cc/FUG2-FURG]; *see also* Letter to Senator Warner, *supra* note 99 ("The COPPA Rule applies not only to websites, but also to other online services, including connected toys and associated mobile apps.").

[106] *See* 15 U.S.C. § 6502 (regulating collection of only information on the Internet). It should be further clarified that if a toy could connect to another device via Bluetooth, then some privacy risks might also rise, as hackers could potentially gain access to these toys.

[107] *Id.*

[108] *See* 16 C.F.R. § 312.2 (2012).

[109] *See* 15 U.S.C. §§ 6501(b)(8), 6502(a)(1).

[110] Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 355, 394 (2011) (internal citation omitted).

[111] 16 C.F.R. § 312.11(a)–(b) (2012); Rubinstein, *supra* note 110, at 395; *see also* 15 U.S.C. § 6503(b)(1) (2012).

the latter, without transparency of FTC-approved practices,[112] this Article focuses on COPPA's five general requirements. Each of these is followed by examples of its being satisfied by key market players in the IoToys market.[113]

The first component is *notice*.[114] This form of regulation-by-information is a well-known practice in many markets.[115] Under it, consumers must be apprised of the various implications of using a product they have purchased or a service they registered to.[116] As COPPA applies to the internet, regulators require that a notice must be posted on the website.[117] A link to the notice must be prominent and clearly labeled, and appear on the home or landing page or screen offering services where personal information is collected from

---

> There are three key criteria for safe harbor approval. Self-regulatory guidelines must (1) meet or exceed the five statutory requirements identified above; (2) include an 'effective, mandatory mechanism for the independent assessment of . . . compliance with the guidelines,' such as random or periodic review of privacy practices conducted by a seal program or third-party; and (3) contain 'effective incentives' to ensure compliance with the guidelines such as mandatory public reporting of disciplinary actions, consumer redress, voluntary payments to the government, or referral of violators to the FTC.

Rubinstein, *supra* note 110, at 395 (citing 16 C.F.R. § 312.11 (2012)); *see also* 15 U.S.C. § 6503 (2012).

[112] While the FTC announced that it approved applications like the iKeepSafe Safe Harbor Program, it is difficult to assess their practices without transparency. *See* Letter from Donald S. Clark, Sec'y, Fed. Trade Comm'n, to Marsali S. Hancock, President & CEO, Internet Keep Safe Coal., *Application of iKeepSafe Safe Harbor Program for Approval of Its Children's Online Privacy Protection Rule Safe Harbor Program* (Aug. 1, 2014), https://www.ftc.gov/system/files/documents/public_statements/573811/140806ikeepsafeapp.pdf [https://perma.cc/4W43-5PU5].

[113] It should be noted that Hello Barbie is currently certified by the FTC as COPPA compliant under the kidSAFE Seal Program. *See infra* note 216. Hence, the use of Hello Barbie is not to imply that it does not comply with COPPA regulation, but rather to exemplify the practices of key-market players within each of the five FIPPs within the regulatory framework.

[114] 16 C.F.R. § 312.3(a) (2012).

[115] Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 650 (2011) [hereinafter Ben-Shahar & Schneider, *Failure*]. Regulation by information refers to a broad type of regulatory mechanisms that rely mostly on the notion that individuals can make more-educated choices when they obtain more information. *Id.* at 649. Under such regulatory mechanism, the "discloser" gives the "disclosee" information, and thus the latter can make better decisions for him, and likewise reduce the "power" of the former to control the latter. *Id.* For examples of disclosure requirements set by legislation, see *id.* at 649–50. For more on regulation through information, see generally OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE (2013) [hereinafter BEN-SHAHAR & SCHNEIDER, MORE] (exploring "Digital Natives" in regards to privacy, creativity, cyber-bullying, and online political activism).

[116] *See* Ben-Shahar & Schneider, *Failure*, *supra* note 115, at 649.

[117] 15 U.S.C. § 6502(b)(1)(A)(i) (2012).

children.[118] The notice must include "what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information."[119] It must also be clear and understandable and in writing,[120] and the OSP must make reasonable efforts to notify parents directly regarding its practices.[121]

Many of the key market players, like ToyTalk, for instance, are found largely to comply with the notice component.[122] ToyTalk posts clear links to its privacy policy and statements on what information is collected, how it is used, and its disclosure practices on both its homepage and the designated webpage for downloading the companion app for both Barbie products.[123] While its evaluation is subjective, it also uses clear and understandable language.[124] Genesis, however, might fulfill this requirement less. Cayla's homepage currently does not contain such a link.[125] Nor does the App Store, when the designated app is downloaded.[126] Cayla's privacy policy is only visible after a user goes to the "More" section on the top menu.[127]

---

[118] 16 C.F.R. § 312.4(d) ("The link must be in close proximity to the requests for information in each such area.").

[119] 15 U.S.C. § 6502(b)(1)(A)(i) (2012).

[120] 16 C.F.R. § 312.4(a) (2012) ("Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.").

> [T] he online notice of the Web site or online service's information practices must state the following: (1) The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the Web site or online service; . . . (2) A description of what information the operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how the operator uses such information; and the operator's disclosure practices for such information; and (3) That the parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

Id. § 312.4(d).

[121] *See id.* § 312.4(b) (requiring operators to "include[e] notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented").

[122] *See, e.g.*, *ToyTalk*, TOYTALK, https://www.toytalk.com [https://perma.cc/2J2J-4YD6].

[123] *Id.*; *Hello Barbie™ Companion App*, https://www.toytalk.com/product/hello-barbie [https://perma.cc/4HS4-U8EY]; *Hello Dreamhouse™ Companion App*, https://www.toytalk.com/product/hello-house [https://perma.cc/B322-H4H7].

[124] *See supra* notes 122–23.

[125] *See Original Cayla*, MY FRIEND CAYLA, https://www.myfriendcayla.com/original-cayla [https://perma.cc/6MPE-ENND].

[126] *See My Friend Cayla App (EN-US)*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.toyquest.Cayla.en_us [https://perma.cc/4ZSS-SL8F]; *My Friend Cayla App*, APP STORE, https://itunes.apple.com/us/app/my-friend-cayla-app-us-english/id1135402140?mt=8 [https://perma.cc/278Y-K7ZF].

[127] *See Original Cayla*, *supra* note 125.

The second component of COPPA requires *verifiable parental consent*,[128] namely more than parents' implied consent, for the collection, use, or disclosure of personal information obtained from children.[129] The parent must receive notice of such use and authorize the "collection, use, or disclosure of the personal information"[130] and must have the option not to consent to disclosure of information to third parties.[131] The steps for verifiable parental consent are vaguely articulated as "*any reasonable effort* (taking into consideration available technology), including a request for authorization."[132] There are some exceptions to the consent requirement. For example, if an OSP uses a child's personal information for internal purposes alone and does not disclose this information, it could obtain consent through the method known as "email plus."[133] In addition, the FTC could approve other methods that satisfy the parental consent requirement.[134]

What should be deemed a reasonable effort in the IoToys realm? Connecting the device, including configuration with the home Wi-Fi, strikes one as insufficient to fulfill this requirement, as COPPA insists on parents' explicit verifiable consent and lists methods such as a signed letter/form, video chat, or phone call with trained personnel.[135] Currently, parental consent for Barbie

---

[128] 16 C.F.R. § 312.3(a)(1) (2012).

[129] 15 U.S.C. § 6502(b)(1)(A)(ii) (2012); 16 C.F.R. §§ 312.2, 312.4–312.5 (2012). There are some exceptions, however, set under 15 U.S.C. § 6502(b)(2) (2012) and 16 C.F.R. § 312.5 (2012).

[130] 16 C.F.R. § 312.2 (2012).

[131] *Id.* § 312.5(a)(2).

[132] 15 U.S.C. § 6501(9) (2012) (emphasis added).

[133] *See* FED. TRADE COMM'N, *supra* note 105. Under this method, the OSP sends an email to the parent and has them respond with their consent. *Id.* The OSP then sends a confirmation to the parent (via email, letter, or phone call). *Id.* OSPs must also notify the parents how to revoke their consent at any given time. *Id.*

[134] 16 C.F.R. § 312.5(b)(3) (2012). Under this safe harbor program, the FTC could determine that the method of the OSP meets the requirements set for verifiable parental consent. *See id.*

[135] *See id.* § 312.5(b)(2). These methods include:

> Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder . . . and [v]erifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete.

Id. § 312.5(b)(2)(ii), (v). If the OSP "does not disclose (as defined by § 312.2) children's personal information," it "may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent." *Id.* § 312.5(b)(2)(vi) ("Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call."). *Id.*

products is obtained by creating an account and accessing ToyTalk services.[136] Genesis merely states that using its website or providing it with any information constitutes consent to the "collection, processing, maintenance and transfer of personal information."[137] It further states: "If you do not agree to this, please do not use our website or provide us with any information."[138] Genesis, however, notes that it "will not knowingly accept any information by any children under the age of [thirteen] without the express permission of their parent and/or guardian."[139]

The third step is *right of parental review*.[140] At a parent's request, OSPs are required to provide the following three things: "(1) A description of the specific types or categories of personal information collected from children by the operator;"[141] "(2) The opportunity . . . to refuse . . . further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information;"[142] and (3) Grant parents the right to review the collected information.[143]

For Barbie products, ToyTalk specifies that parents have the right to review or delete any personal information collected from their child that it retains.[144] Parents also have the "right to review and delete" any audio files in their account and "may also permanently delete their accounts via ToyTalk's website."[145] Even lacking a request, ToyTalk claims that it will delete personal information that children provide when it "becomes aware of it, and [it] will contractually require [its service] providers" to act similarly.[146] For Cayla, Genesis claims that parents have the right to ask not to process their personal information for marketing purposes, the right to ask to update their records or delete any personal information the company holds about them (but mentions that it "may need to keep that information for legitimate business or legal purposes"), and

---

[136] *See* TOYTALK, *Privacy*, *supra* note 54 ("Unless Barbie Products are used only in offline mode, we obtain parental consent for the use of the Service using an approved method under the Children's Online Privacy Protection Act ('COPPA'). By creating an account and accessing the Services, you are certifying that you are authorized to provide such consent and responsible for all activities under the account.").

[137] *See Privacy Policy*, GENESIS TOYS, https://www.genesis-toys.com/privacypolicy [https://perma.cc/NM2C-7RHE] (last updated Feb. 23, 2015).

[138] *Id.*

[139] *Id.*

[140] 16 C.F.R. § 312.3(c) (2012).

[141] *Id.* § 312.6(a)(1). Examples are "name, address, telephone number, email address, hobbies, and extracurricular activities." *Id.*

[142] *Id.* § 312.6(a)(2).

[143] To comply, considering available technology, OSPs must "[e]nsure that the requestor is a parent of that child" and that the means "not be unduly burdensome to the parent." *Id.* § 312.6(a)(3)(i)–(ii).

[144] TOYTALK, *FAQ*, *supra* note 60.

[145] *Id.*

[146] *Id.*

the right to access information it holds about them.[147] Essentially, these practices comply with the third step of COPPA regulation.

The fourth step requires scrutiny of whether OSPs "condition a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity."[148] This step might be trickier with respect to IoToys than to websites. Arguably, regarding toys, almost every activity could be viewed as imposing conditions and disclosure of data on the child's participation. Also, while not all data will be deemed personal information, many data might.[149] The difficulty in IoToys, however, would be assessing whether such disclosure is "necessary to participate in such activity," and more closely, whether it is reasonable.[150] Practically, without disclosure of the datamining practices of OSPs and scrutiny of how personal information is linked to the child's participation, it is difficult to examine how companies comply with this requirement.

The final evaluation step is whether OSPs maintain *reasonable security policies*.[151] OSPs are obliged to "[e]stablish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[152] Releasing the information to a third party requires ensuring that the third party takes similar steps to protect the data and can vouch for these measures.[153] To reduce the risk of privacy violations in a cybersecurity breach, the FTC also imposes on OSPs "[d]ata retention and deletion requirements."[154]

Surveys have shown that many IoToys OSPs implement data security measures in their toys.[155] Barbie products use secure, encrypted communications when transferring all personal information over the web.[156] Wi-Fi credentials are stored in an encrypted section so that the products can connect to the internet.[157] The Hello Barbie Hologram uses 256-bit encryption

---

147 *See Privacy Policy*, *supra* note 33.

148 16 C.F.R. § 312.3(d) (2012).

149 *Id.* § 312.2.

150 *Id.* § 312.3(d).

151 *Id.* § 312.3(e).

152 *Id.*

153 *Id.* § 312.8; *see also* CHILDREN'S CONNECTED TOYS, *supra* note 57, at 6 ("If the operator transfers children's personal information to a third party, the operator must also ensure that the third party has taken similar steps to protect the data.").

154 16 C.F.R. § 312.10 (2012).

155 CHILDREN'S CONNECTED TOYS, *supra* note 57, at 9. These measures include but are not limited to "firewalls; user restrictions, access controls, and authentication procedures; remote access through an encrypted VPN tunnel; monitoring networks for unauthorized activity; regular updates and patches to software; vulnerability testing; and engaging independent security services to test systems for vulnerabilities." *Id.*

156 TOYTALK, *Privacy*, *supra* note 54.

157 *See id.*

when it sends queries to the cloud.[158] For Cayla, Genesis claims that it undertakes internal reviews of its data management, including "appropriate encryption and physical security measures to guard against unauthorised access to systems where we store personal information."[159]

Are these security policies reasonable? Difficult to say, as it depends on the toy in question.[160] But in practice they are found not secure enough: IoToys has often been breached since its inception,[161] including Hello Barbie.[162] Another problem is that under the current regulatory framework, the reasonableness of the security measures will usually be evaluated *ex post*, mostly after a data

---

[158] *See* Moynihan, *supra* note 40. It should be noted that Aristotle was supposed to use encryption to keep at least some form of information private. *Aristotle*, QUALCOMM (Jan. 3, 2017), https://www.qualcomm.com/media/documents/files/mattel-s-nabi-brand-introduces-first-ever-connected-kids-room-platform-in-tandem-with-microsoft-and-qualcomm.pdf [https://perma.cc/K5Z4-ZZCT]. Mattel claimed that they encrypt every piece of data using AES 256-bit end-to-end symmetric key encryption and create a unique device-to-device key to ensure safety of data streams. *Id.*

[159] *Privacy Polic*y, *supra* note 33.

[160] For an analysis of security flaws in IoToys, see Valente & Cardenas, *supra* note 51, at 19.

[161] *See, e.g.*, Lorenzo Franceschi-Bicchierai, *One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*, VICE MOTHERBOARD (Nov. 27, 2015), http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids [https://perma.cc/Q8XM-58YB] (describing a breach of consumer data to VTech Electronics North America, a maker of children's connected tablets); Alex Hern, *CloudPets Stuffed Toys Leak Details of Half a Million Users*, THE GUARDIAN (Feb. 28, 2017), https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults [https://perma.cc/4VUM-4TDE] (describing a data breach that compromised personal information of more than half a million people who bought the toys); Mark Stanislav, *R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy® & hereO GPS Platform Vulnerabilities (FIXED)*, RAPID7 (Feb. 2, 2016), https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform [https://perma.cc/Z783-Q7P2]; Danny Yadron, *Fisher-Price Smart Bear Allowed Hacking of Children's Biographical Data*, THE GUARDIAN (Feb. 2, 2016), https://www.theguardian.com/technology/2016/feb/02/fisher-price-mattel-smart-toy-bear-data-hack-technology [https://perma.cc/JNE3-SA6G] (noting that the app connected to the Fisher-Price toy had several security flaws that would allow hackers to obtain data).

[162] Samuel Gibbs, *Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children*, THE GUARDIAN (Nov. 26, 2015), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children [https://perma.cc/GVA8-UTMK] (showing how hackers hijacked a Hello Barbie); *see also* Richard Chirgwin, *Hello Barbie Controversy Re-Ignited with Insecurity Claims*, THE REGISTER (Nov. 29, 2015), http://www.theregister.co.uk/2015/11/29/hello_barbie_controversy_reignited_with_insecurity_claims [https://perma.cc/4M25-AQGD] (discussing Hello Barbie's potential to be hacked). Another example is that of "Furby hacking," i.e., hacking into the toy Furby and manipulating it. This widely-known hobby dates back to the toy's original release in 1998. Darren Orf, *Hackers Found a Way to Make Furbies Even Creepier*, GIZMODO (Feb. 9, 2016), http://gizmodo.com/hackers-found-a-way-to-make-furbies-even-creepier-1756683110 [https://perma.cc/FW5S-KV5Z].

breach.[163] A recent example concerns VTech Electronics Limited, an electronic toy manufacturer, which experienced a major cybersecurity breach.[164] Only then did consumers learn that their children's data was not encrypted even though the firm's privacy policy stated that it was.[165]

Whether OSPs generally comply with COPPA is disputable. With some exceptions for actions subject to legal interpretation, most of the key market players probably comply with most of COPPA requirements, at least in their narrowest sense. Bearing in mind the FTC's enforcement prerogative, one would presume that at least the key players will comply with the default requirements of COPPA in the absence of any substantial market failures. Nevertheless, compliance with COPPA does not mean that COPPA in its current form properly safeguards children's privacy within the realm of IoToys. As the next Part shows, the transition from the internet to IoToys necessitates a reevaluation of COPPA as to whether it is the optimal mechanism to protect children's privacy online; a recalibration of COPPA in light of IoToys's challenges is suggested.

IV. REEVALUATING AND RECALIBRATING CHILDREN'S PRIVACY

While it may be disputable whether IoToys OSPs currently comply with COPPA regulation, the broader normative question is whether COPPA regulation adequately meets the challenge of IoToys. This is not to argue that COPPA must be directed towards a specific technology or a sector (unlike a cohort, as currently crafted), but rather that the implications of COPPA—through the examination of new technologies—might suggest broad implications on the perception of American privacy regulation. Accordingly, this Part assesses how to protect children's privacy in IoToys under the current American framework. The argument proceeds in two stages: the first differentiates regular online activities from activities within the IoToys realm as regards regulating children's privacy. It maintains that fundamental differences between the two require policymakers to recalibrate the regulatory framework that governs children's privacy. The second stage offers insights into such recalibration, while revisiting COPPA's five essential incorporated FIPPs by suggesting practical adjustments to COPPA regulation in the IoToys realm.

---

[163] *See* Press Release, Fed. Trade Comm'n, Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated [https://perma.cc/K7SQ-TBPG].

[164] *See id.*

[165] *See id.* VTech eventually settled with the FTC and was obliged to pay $650,000 for a COPPA violation. *Id.*

A. *Revisiting Children's Privacy in IoToys*

The common purpose of regulating conduct that relates to both the internet and IoToys is obviously to provide safeguards for children against potential harms, mainly risks to their informational privacy. On the other hand, a one-size-fits-all approach may be inappropriate, as key differences may exist between the internet and IoToys regarding children's privacy interests. While IoToys depends on the internet, its implications for children's privacy are not necessarily synonymous with visiting websites.

COPPA was crafted in an era when policymakers sought to protect the privacy of personal information collected from and about children on the World Wide Web.[166] The need to protect children's privacy in IoToys not only exists but is actually greater.[167] It is based on the core differences between the internet and IoT in general, where IoT "increase[s] the number of vulnerabilities that could potentially be exploited to conduct" unlawful activities; it increases the amount of data collected on individuals and thereby increases the chances of privacy violations; and it reduces the capacity to control the vast amount of information.[168] More closely, IoToys's design, or stated differently, architecture, affects the *volume* of data gathered, its potential *variety*, and *access* to it.

IoToys broadens the *volume* of children's data due to various factors. As a rather intuitive argument, it does so simply by adding another form of connection to the internet. Arguably, however, children might view IoToys devices as substitute goods for websites, that is, essentially they will merely replace data that might have been shared online with data that is shared with the toy. But it is hard to see these two different forms of children's play as basically the same, as they sometimes perform different functions and might appeal differently at least to some children. The two might offer different types of interaction or play, hence they are unlikely to be considered interchangeable (substitute) goods for all children.

More closely, IoToys expands the volume of data as it widens the target audience by increasing accessibility to it. IoToys shifts the form of communication from writing (typing) to talking, thereby making the toys accessible to a wider cohort of children who are otherwise unable to use a computer or browser, or simply cannot yet read or write.[169] This relates not only to younger children, but also to other children who experience difficulty writing or reading. These toys offer them increased access to the internet.

---

166 *See* 16 C.F.R. § 312.1 (2012).

167 *See* Shackelford et al., *supra* note 1, at 427.

168 *Id.*

169 Notably, however, IoToys might be more challenging than the internet for children that experience hearing impairment or speech impediments.

Another factor that increases volume is computer or technological illiteracy.[170] As a core argument, children, at least young ones, might be more accustomed to playing with toys than using a computer; hence, IoToys devices will appeal to them more and be generally easier to use. Notably, however, this argument might become less relevant for digital natives,[171] as the use of computers like smartphones or tablets might begin at relatively early stages of their lives.[172] Still, after the setup step, usually undertaken by the child's parent, operating IoToys devices like Hello Barbie or Cayla is generally easier and quicker than using the internet via computers. Perhaps IoToys devices might also be more enjoyable, hence, the gamification by itself increases the volume of data.

Volume could also be linked with mobility. Computers are not naturally limited physically to remote rooms of a house, and laptops, mobile phones, tablets, and other potential connected devices can also connect to the internet. Nevertheless, parents might decide to limit their children's accessing the internet, especially young ones, to a computer that is fairly visible to the parents. IoToys devices' mobility, however, is different due to the toys' architecture. They can be used wherever the children want, as long as an internet connection is available.[173] Thus, the mere fact that these devices are generally more mobile than traditional computers can increase children's access to the internet and increase the volume of gathered data.

Finally, volume of data could also be under parental control—less as regards the physical space than the gathered information. On the internet, parents can sometimes use self-management tools—also known as Privacy-Enhancing

---

[170] Computer illiteracy usually refers to the lack of knowledge and ability a person has to use computers, while technological illiteracy refers to reduced knowledge on the handling and use of technological tools, including computers but also internet use. For further reading on these definitions, see Randall S. Davies, *Understanding Technology Literacy: A Framework for Evaluating Educational Technology Integration*, 55 TECHTRENDS 45, 46–47 (2011).

[171] While these definitions evolve over time, "digital natives" generally refers to those who grew-up in the digital age, as opposed to "digital immigrants." For more on these terms, see Marc Prensky, *Digital Natives, Digital Immigrants Part 1*, 9 ON HORIZON 1, 1 (2001). *See generally* JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008) (discussing the implications of the first digital natives coming of age).

[172] *See* Jacqueline Howard, *Kids Under 9 Spend More than 2 Hours a Day on Screens, Report Shows*, CNN (Oct. 19, 2017), https://edition.cnn.com/2017/10/19/health/children-smartphone-tablet-use-report/index.html [https://perma.cc/CXF7-BPS6]. As reported by Common Sense Media, a nonprofit organization, in 2017, 42% of American children aged eight or younger had their own tablet devices. *Id.*; *see also* David Nagel, *One-Third of U.S. Students Use School-Issued Mobile Devices*, THE JOURNAL (Apr. 8, 2014), https://thejournal.com/articles/2014/04/08/a-third-of-secondary-students-use-school-issued-mobile-devices.aspx [https://perma.cc/2YMU-CFH3] (discussing the prevalence of technology access among children).

[173] *See supra* note 27 and accompanying text.

Technologies (PET)—designed to enhance users' privacy.[174] We also encounter other filtering software as a partial solution to online dangers, indeed, perhaps above all, to limit children's ability to access websites or provide personal information.[175] While these are far from a perfect solution to regulate children's online behavior, the IoToys market is more complex. Once a toy is in use, it is difficult for parents to control what their children are doing at any given time if the OSP does not provide them with privacy setting tools. Thus, the ability to control or block access might be more limited without such self-management tools, consequently the volume of the shared data might rise.

Regarding the data's *variety*, if the toy seems trustworthy from a child's perspective, he or she might also share diverse information with it, which might also be more sensitive. Toys in general might seem harmless from a child's perspective. Children might, for instance, conceive their toy to be their new best friend and form an attachment.[176] Children might even anthropomorphize these toys, that is, become convinced that they are human, which might lure them to disclose data that is sensitive, at least from their own perspective (like secrets).[177] Naturally, however, this aspect could be challenged to the extent that IoToys might also be more limited in the types of gathered data. By this argument, websites could be more diverse in the types of interactions offered, thus could consequently extract a wider variety of data from their users. It could also be further challenged that anthropomorphizing these toys might actually lead to children not trusting them, or rather, telling them lies. Still, along with developments in IoToys devices, their ability to offer more types of interactive

---

[174] *See generally* Ian Goldberg et al., *Privacy-Enhancing Technologies for the Internet*, PROCEEDINGS OF IEEE COMPCON '97 103 (1997) (overviewing PETs). Good examples of PETs are communication anonymizers and Enhanced Privacy ID (EPID), digital signature algorithms supporting anonymity. Other examples include the Platform for Privacy Preferences (P3P) designed to provide "smarter Privacy Tools for the Web." *Platform for Privacy Preferences (P3P) Project*, W3C (Oct. 3. 2007), https://www.w3.org/P3P [https://perma.cc/WWF9-BB4X]. Essentially, P3P is a protocol that allows websites to declare their intended use of information they collect. *See id.* A final example is the *TrackMeNot* browser plug-in, which "send[s] 'decoy' queries to popular search engines . . . whenever a user searches" them while generating "algorithmically generated 'noise.'" Daniel C. Howe, *Surveillance Countermeasures: Expressive Privacy via Obfuscation*, INTERARTIVE (June 2016), https://interartive.org/2016/06/surveillance-countermeasures-expressive-privacy-via-obfuscation-daniel-c-howe [https://perma.cc/J29E-Z3JL].

[175] Examples in the early 2000s included computer programs like Cybersitter and NetNanny. Hertzel, *supra* note 69, at 447–48.

[176] *See* Vlahos, *supra* note 15. Upon initiation, Hello Barbie explicitly communicates that to the user. *Id.* Upon asking the child's name, Hello Barbie replies, "I just know we're going to be great friends." *Id.*

[177] *See id.* Professor Doris Bergen argued that it is very difficult for children, especially young ones, "to distinguish what is real from what is not real." *Id.*; *see also* Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 787 (2015) (arguing that young children might become attached to robots "acting autonomously" and "disclose secrets that they would not tell their parents or teachers").

games will not be more limited than websites and will most likely continue to expand.

The final aspect is *access* to the toy and the stored data. For its evaluation, access should be divided between authorized and unauthorized. In terms of authorized access, the data gathered through websites and IoToys devices should not differ greatly, depending on their marketing purposes. Unauthorized access, however, is generally facilitated in IoToys due to potential security flaws.[178] Indeed, it is difficult to assess the differences between the security of websites and of IoToys in general. On the whole, IoToys and websites could greatly differ in their cybersecurity measures. The difference would mainly be that IoToys's data storage is divided into three hackable methods to obtain data (through the toy, the app, or the cloud), while websites can rely on a single database.[179] Thus, the insecurity of children's data in IoToys may be greater simply because there are more ways of obtaining it.

The differences between the *volume* of data gathered, its potential *variety*, and *access* to it imply that IoToys can gather more information than the internet can and that this information might be more sensitive and less secure. These differences could essentially lead to higher risks to children's privacy. To mitigate these risks within the COPPA framework, policymakers must revisit and recalibrate parents' self-management of their children's privacy, the OSP's requirements, and public enforcement of IoToys.

B. *Recalibrating the Legal Framework*

COPPA fails to regulate IoToys properly. While the FTC has amended the COPPA rule and has issued further guidelines for parents as well as OSPs in the IoToys market, regulating IoToys requires acknowledging the differences between it and the internet.[180] Examining the current COPPA requirements in light of these differences clearly shows how inadequate COPPA is to properly safeguard children from privacy risks. This inadequacy must be further addressed by recalibration.

As a general matter, one might argue that the legal framework of sectoral privacy in general is no longer applicable in this age and that the United States should take the path chosen by the European Union and embrace an omnibus privacy regime.[181] One might argue that it is not wise to keep updating laws such as COPPA due to the rise of new technologies, but rather craft technology-

---

[178] *See generally* Valente & Cardenas, *supra* note 51 (analyzing IoToys's security systems).

[179] *See id.* at 19–21 (mentioning three data entry points).

[180] *See supra* notes 82, 105, and accompanying text.

[181] *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1762 (2010). *But see* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 946 (2009) (discussing the drawbacks of embracing an omnibus privacy regime in the United States).

neutral laws.[182] While such moves could very well be advisable, this Article will not undertake this important theoretical debate but will rather pragmatically focus on the current approach to American privacy and examine its current applicability.

But before suggesting how COPPA should be recalibrated, it is crucial to rule out other potential legal measures currently set in the United States to allay these risks. For instance, the potential constitutional protection of children's privacy will not advance the discussion on IoToys much. Privacy is often interpreted as a right that could be located within various constitutional amendments such as the Fourth Amendment,[183] but by its present interpretation of the Supreme Court, it will not extend to non-state actors, which include IoToys manufacturers and OSPs, so information privacy will generally not be protected by it.[184] Accordingly, tort law will be fairly limited in dealing with the risks of IoToys as it mainly concerns disclosure of embarrassing personal information and not simply the collection and use of personally identifiable information.[185] Consumer protection law could be invoked to some extent, but it will mainly deal with the IoToys device itself, and less with the practices of safeguarding the stored data, at least on the federal level.[186]

---

[182] For more on technology-neutral legislation, see generally Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J.L. & TECH. 24 (2012).

[183] *See* U.S. CONST. amend. IV.

[184] Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 502 (1995). As interpreted by the Supreme Court, the Bill of Rights grants implicit constitutional protection for privacy. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 152 (1973); Griswold v. Connecticut, 381 U.S. 479, 484–85 (1964). Examples of this protection include prohibiting unreasonable searches and seizures and protecting freedom of assembly. U.S. CONST. amends. I, IV. Invoking constitutional rights, however, requires that a state action be present. Reidenberg, *supra*, at 502. Thus, these rights protect citizens against the government, while they fail to grant protection for citizens against each other (including against private companies); *see id.* at 501–03.

[185] *See* RESTATEMENT (SECOND) OF TORTS § 652 (AM. LAW INST. 1977). As described by Professor William L. Prosser, the right to privacy could be protected to some extent by tort law under four branches: "(1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) Public disclosure of embarrassing private facts about the plaintiff; (3) Publicity which places the plaintiff in a false light in the public eye; [and] (4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness." William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). Establishing a tort claim under these branches in IoToys will be difficult in most instances as misappropriation protects only against the unauthorized use of a person's name or likeness for commercial purposes, Prosser, *supra*, at 401–07, public disclosure of private facts protects against the circulation to the general public of offensive information (that is not otherwise publicly available), *Id.* at 392–98, and false light protects against wide dissemination of information that is misleading or erroneous, *Id.* at 398–401. What might be relevant is intrusion upon seclusion, which protects against highly offensive methods of gathering information in private areas. *Id.* at 389–92. For more on torts and privacy, see Reidenberg, *supra* note 184, at 504–06, and Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1291 (2000).

[186] For more on consumer protection law in the United States, see generally Spencer Weber Waller et al., *Consumer Protection in the United States: An Overview*, EUR. J.

COPPA regulation is not the sole component of the current regulatory framework that potentially protects children's privacy from the risks of IoToys. Still, it is highly improbable that other legal measures could be invoked in the IoToys context or be sufficient to protect children's privacy. An obvious *ex ante* solution for not only reducing the potential risks of IoToys devices but also removing them altogether would be for policymakers to simply ban their manufacture, import, and even use. This solution might not be as farfetched as it might sound. When Furby was first introduced in 1998, the National Security Agency banned it out of fear that it might record classified conversations.[187] In the IoToys market, German authorities embraced this approach recently when they decided to ban the IoToys device Cayla due to its (proclaimed) inherent security flaws.[188] Germany's Federal Network Agency even took this approach a step further and classified Cayla as an "illegal unlicensed radio device," meaning that parents who possessed this doll might be prosecuted and face up to two-years imprisonment for possessing a banned surveillance device.[189]

This Article does not support such solutions as an agenda, and they are also highly unlikely in the United States. Beyond the potential benefits to children, IoToys could be valuable for technological developments and innovation.[190] This solution might negatively affect the progress of knowledge as flow of information could enhance innovation. Datafication could develop technology for analysis and "business models to utilize the derived information,"[191] and it could further "lead to social benefits and the enhancement of social welfare."[192] Thus, heavily regulating the flow of information, let alone banning IoToys devices altogether, could stifle innovation and should be carefully examined.[193]

Instead of banning IoToys, policymakers should consider other less-restrictive legal measures, which could lessen the risks that IoToys entails while preserving its benefits. To achieve such a balance, policymakers must combine

---

CONSUMER L. (May 2011), https://ssrn.com/abstract=1000226 [https://perma.cc/4N6Q-P34B] (surveying the United States regulatory framework for consumer protection).

[187] *World: Americas: Furby Toy or Furby Spy?*, BBC NEWS (Jan. 13, 1999), http://news.bbc.co.uk/1/hi/world/americas/254094.stm [https://perma.cc/4NXZ-B7HY].

[188] Dakshayani Shankar, *Germany Bans Talking Doll Cayla over Security, Hacking Fears*, NBC NEWS (Feb. 18, 2017), http://www.nbcnews.com/news/world/germany-bans-talking-doll-cayla-over-security-hacking-fears-n722816 [https://perma.cc/9L5W-6TKX].

[189] *Id.* Notably, Germany also recently banned children's smartwatches. Jane Wakefield, *Germany Bans Children's Smartwatches*, BBC NEWS (Nov. 17, 2017), http://www.bbc.com/news/technology-42030109 [https://perma.cc/J899-TLG6].

[190] For a comprehensive analysis of the privacy-innovation debate, see Tal Z. Zarsky, *The Privacy-Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 119–21 (2015). In the context of big data, see Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1918–27 (2013).

[191] Zarsky, *supra* note 190, at 118.

[192] *Id.*; *accord* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 243–51 (2013).

[193] *See* Zarsky, *supra* note 190, at 118 n.5, 119.

ex ante and *ex post* measures, by allowing developments in IoToys, while setting a framework in which these toys operate, are manufactured, and are sold, and especially how, by whom, and for which purposes data are used. Essentially, COPPA regulation attempts to do precisely this, but as previously mentioned, it requires far-reaching modifications to its requirements.

1. *Raising Awareness*

Any legal guardian, even without purchasing IoToys devices, must be aware of their potential implications. They must certainly understand the risks of IoToys to information privacy and security by understanding the information the OSP collects, "how that information will be used," "whether it will be shared," and if so with whom, and "how long the information will be retained."[194] Parents and guardians must assume a position enabling them to make educated decisions regarding their children's privacy. They have to be aware of these toys' implications, as their children might also become secondary users, namely by playing with an IoToys device without their parents' knowledge or consent.[195]

Awareness can be promoted in various ways. One way is to reduce information gaps through regulation-by-information. Under this regulatory approach, toy manufacturers and OSPs will be obliged to apprise consumers of IoToys's privacy risks, thereby reducing the disclosers' power to control the disclosees by granting them informed choice on whether to use these

---

[194] *See* CHILDREN'S CONNECTED TOYS, *supra* note 57, at 2.

[195] The notions of awareness and consent in IoToys might be also perceived as tricky due to secondary users. What happens, for instance, when a child uses his friend's IoToys device, consented for use only by the parent of the friend? Indeed, a class action revolving secondary users in Hello Barbie was filed against ToyTalk, Inc. and Mattel in the California Superior Court. The class action alleged, inter alia, that OSPs violated COPPA as the IoToys device captured the voices of other children whose parents had not consented (Hello Barbie recorded conversations of the plaintiff while attending a friend's birthday party). Notice of Removal at 1, 2, Archer-Hayes v. Toytalk, Inc., No. 2:16-cv-02111-JAK-PLA (C.D. Cal. Mar. 29, 2016). From a legal certainty perspective, this case was unfortunately voluntarily dismissed, leaving void the applicability to secondary use within IoToys. *See* Stipulation of Voluntary Dismissal with Prejudice at 1, Archer-Hayes v. Toytalk, Inc., No. 2:16-cv-2111-JAK-PLA (C.D. Cal. July 22, 2016). It is generally still unclear whether a secondary use of an IoToys device will be deemed as personal identifiable information under COPPA, as an unnamed and unidentified voice is not necessarily "personal information" (unlike the child who owns the toy). Practically, if we take ToyTalk's privacy policy as an example, allowing other people to use the service via their account is considered a confirmation of the right to consent on their behalf to ToyTalk's collection, use, and disclosure of their personal information. Alex B. Lipton, Note, *Privacy Protections for Secondary Users of Communications-Capturing Technologies*, 91 N.Y.U. L. REV. 396, 406 (2016) ("By allowing other people to use the Service via your account, you are confirming that you have the right to consent on their behalf to ToyTalk's collection, use and disclosure of their personal information as described below." (quoting *Privacy Policy Terms of Use FAQ*, TOYTALK, https://toytalk.com/hellobarbie/privacy/ [https://perma.cc/A6XC-59SM]).

products.[196] While COPPA promotes this type of regulation by its notice requirement,[197] it generates insufficient awareness regarding IoToys, as it fails to acknowledge the difference between using a website and playing with a toy. Merely placing a notice on a website will hardly raise awareness.[198] When the internet is embedded in the operation of devices, direct exposure to a website does not exist, even if OSPs maintain one. Thus, the existence of a notice in a website regarding the collection, retention and use of information does little in itself to detail the rationale behind the notice requirement. The notice must appear on the toy's packaging and on online platforms like the app that is used to set up the toy. But on its own, this requirement is still insufficient to properly raise awareness.

One of the main problems of the notice requirement in terms of awareness concerns the known practice of confusing users with long and incomprehensible policies. Regarding IoToys, the FBI advises parents to carefully read disclosures and privacy policies.[199] But practice shows that this is unlikely to occur. As may be drawn from terms of service (ToS) agreements and end-user license agreements (EULAs),[200] most consumers do not bother to read them[201] and they are usually long, broad,[202] and written in a legal language almost incomprehensible to most people, as are privacy policies or notices.[203] Most

---

[196] *See generally* BEN-SHAHAR & SCHNEIDER, MORE, *supra* note 115 (arguing that mandated disclosures are ineffective); Ben-Shahar & Schneider, *Failure*, *supra* note 115 (discussing the historical use of mandated disclosures).

[197] 16 C.F.R. § 312.3(a) (2012).

[198] As currently regulated under COPPA and codified at 15 U.S.C. § 6502(b)(1)(A)(i) (2012).

[199] *See Consumer Notice: Internet-Connected Toys Could Present Privacy Concerns for Children*, FED. BUREAU OF INVESTIGATION, INTERNET CRIME COMPLAINT CTR. (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx [on file with *Ohio State Law Journal*].

[200] The use of ToS and EULAs are merely to exemplify how individuals treat vast amounts of information online. It should be stressed that this Article does not argue that these agreements are similar to privacy policies. While terms of use are the province of contract law, privacy policies seem currently to be mainly the province of the FTC. *See* Solove & Hartzog, *supra* note 83, at 589. For attempts to enforce privacy policies as contracts, see, for example, *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316–18 (E.D.N.Y. 2005); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1199–1200 (D.N.D. 2004).

[201] *See* Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 930 (2013); Ben-Shahar & Schneider, *Failure*, *supra* note 115, at 665–78; Solove, *supra* note 88, at 1885.

[202] *See, e.g.*, Garry L. Founds, *Shrinkwrap and Clickwrap Agreements: 2B or Not 2B?*, 52 FED. COMM. L.J. 99, 100 (1999); Daniel B. Ravicher, *Facilitating Collaborative Software Development: The Enforceability of Mass-Market Public Software Licenses*, 5 VA. J.L. & TECH. 11, 12 (2000).

[203] For studies on privacy notices, see, for example, NISSENBAUM, *supra* note 77, at 105; Annie I. Anton et al., *Financial Privacy Policies and the Need for Standardization*, 2 IEEE SECURITY & PRIVACY 36, 42–44 (2004); Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543 (2008); George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15, 20–21 (2004); Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW

people do not see, read or understand them, and they might also be changed frequently.[204] Even shortening these policies might only insert marginal improvements to make them more comprehensible,[205] and they might also leave out important information to make any consent truly informed.[206] Essentially, individuals already experience information flooding and are unlikely to spend time or effort on reading these polices.[207]

Even if parents do receive full information on IoToys practices, privacy self-management—at least in its current form—is insufficient to raise awareness efficiently.[208] It is beset with cognitive failures and structural problems such as impediments to the parents' ability to adequately assess the costs and benefits of the information they receive.[209] Thus, information is generally substantially insufficient to reduce these risks. Cognitive abilities are required to understand something that may be highly complex in terms of informational privacy.

Within this regulatory framework, at the very least COPPA must be more precise. Assuming that the policy of these OSPs permits collection and sharing of information, they must be obliged to be concise and clear on how information is used and by whom.[210] A clear and understandable notice on how OSPs use

---

RES. CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is [https://perma.cc/FD92-3XD5].

[204] Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 485, 491 (2015); *accord* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160 (1999) ("No one has the time or patience to read through cumbersome documents describing obscure rules for controlling data."); Ohm, *supra* note 201, at 930; Solove, *supra* note 88, at 1885.

[205] *See, e.g.*, M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1032–33 (2012).

[206] *See* Solove, *supra* note 88, at 1885.

[207] *See* Cass R. Sunstein, *Empirically Informed Regulation*, 78 U. CHI. L. REV. 1349, 1369 (2011) ("[E]ven accurate disclosure of information may be ineffective if the information is too . . . overwhelming to be useful."); *see also* Karen Bradshaw Schulz, *Information Flooding*, 48 IND. L. REV. 755, 756 (2015) (describing the cause of "information overload").

[208] *See* Solove, *supra* note 88, at 1883–93.

[209] As suggested by Professor Daniel Solove, cognitive problems arise from four aspects:

> (1) [P]eople do not read privacy policies; (2) if people read them, they do not understand them, (3) if people read them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decisionmaking difficulties.

Id. at 1888.

[210] It should be insufficient to declare that information might be shared "with third-parties" without listing who these third-parties are and what the purpose of this information sharing is. For more on the problem of vagueness, see Reidenberg et al., *supra* note 204, at 518–19. Relating to their smart bear toy, Fisher-Price mentions on their website that "NO PERSONALLY IDENTIFIABLE DATA is transmitted by Smart Toy." Yadron, *supra* note 161 (describing how the toy was able to be hacked, revealing personal information about users).

such information,[211] and their disclosure practices, must be prominently visible to anyone purchasing the toy; also, parents should be reminded of these matters periodically by accessible communication means such as email. The notice must explicitly spell out the potential risks to users when agreeing to the policy.[212] Any vendor of these toys must first make sure that parents understand the risks, and what they are consenting to, at the point of sale.[213]

Furthermore, sellers should be obliged to place simplified and clear privacy labels on the package.[214] Beyond lucid warnings on IoToys devices' packaging, it would be efficient to clearly signal how the toys protect privacy and comply with COPPA. Under this program, OSPs that implement sufficient measures to protect children's privacy should be encouraged to display a privacy seal on the toy. This solution exists in the market, as toys can be certified "COPPA compliant" by the FTC or other organizations, for example, by the kidSAFE Seal Program—a children's privacy certification program approved by the FTC.[215] Hello Barbie is currently a member of such a program.[216] While not perfect, seal programs are generally an efficient method to alert consumers to the potential risks of IoToys devices that do not have such a seal.[217] It could

---

[211] The United States Senate Committee on Commerce, Science, and Transportation advised the FTC to suggest that toymakers will be required to "use clear, plain language to inform parents about the information the toys collect and how that information is used." CHILDREN'S CONNECTED TOYS, *supra* note 57, at 2.

[212] *See* Steinberg, *supra* note 28; *see also* CHILDREN'S CONNECTED TOYS, *supra* note 57, at 15 ("Toymakers should also disclose in plain language the information that is collected from or about a child instead of burying it in their privacy policies."); *cf.* Lobosco, *supra* note 12 (quoting a Mattel spokeswoman that Hello Barbie conforms to COPPA).

[213] *See* KIDS & THE CONNECTED HOME, *supra* note 4, at 13.

[214] *See* Steinberg, *supra* note 28; *see also* CHILDREN'S CONNECTED TOYS, *supra* note 57, at 15 (suggesting that providing the basics of what information is collected and how it is used conspicuously and in clear terms on a toy's packaging would allow parents to be more informed about their children's privacy and security).

[215] The kidSAFE Seal Program is designed for children-friendly websites and technologies, including "online game sites, educational services, virtual worlds, social networks, mobile apps, tablet devices, connected toys, and other similar online and interactive services." The service includes a list of products that meet their online safety and/or privacy standards. *About Our Program*, SAMET PRIVACY, LLC, KIDSAFE® SEAL PROGRAM, https://www.kidsafeseal.com/aboutourprogram.html [https://perma.cc/H3LX-RRLR]. One of the seals is an FTC-approved COPPA certification program called the "kidSAFE+ COPPA" seal. Beyond basic safety rules, this seal has six additional requirements: "Neutral age questions, Parental notice and consent procedures, Parental access to child's personal information, Data integrity and security procedures, COPPA-compliant privacy policy, [and] COPPA oversight and enforcement by the kidSAFE® Seal Program." *About Our Seals*, SAMET PRIVACY, LLC, KIDSAFE® SEAL PROGRAM, https://www.kidsafeseal.com/aboutourseals.html [https://perma.cc/82HW-4VBR].

[216] *Official Membership Page*, SAMET PRIVACY, LLC, KIDSAFE® SEAL PROGRAM, http://www.kidsafeseal.com/certifiedproducts/toytalk_hellobarbie_device.html [https://perma.cc/4LF8-4W7D] (noting that Hello Barbie is kidSAFE+ COPPA certified).

[217] Compare with TRUSTe, a nonprofit organization, "the first online privacy seal program" in the United States. FED. TRADE COMM'N, *supra* note 90, at 6; Hertzel, *supra* note

promote consumer trust, thereby persuading consumers to purchase only IoToys devices that meet FTC standards.

The state, too, should promote awareness. Policymakers must invest in heightening awareness of the potential implications of IoToys. As previously noted, it is crucial for all legal guardians to understand the ramifications of playing with an IoToys device, as their children might become secondary users.[218] The state should therefore invest in advertisements and other forms of education that clearly explain their potential risks.[219] One such effort that could be improved is the FBI's consumer notice for internet-connected toys, which warns of potential risks to children's privacy.[220] While important, the FBI's suggested steps are unlikely be taken by average parents, even if they are exposed to the warnings.[221] Thus, raising awareness must be more meaningful and use practical forms of communication to advise the general public on the privacy risks of IoToys. Still, even awareness will be fairly limited to properly regulate IoToys.

2. *Redefining Choice*

Being alerted to and comprehending the risks, parents should be able to decide whether to consent to the practices that IoToys entails. COPPA currently promotes exercising "*verifiable parental consent*."[222] Generally, this form of privacy self-management is insufficient for IoToys.[223] The efficacy of a notice and choice mechanism has largely been contested because, inter alia, it can uninform or misinform consumers,[224] it is "impractical" and ineffective,[225] and

---

69, at 445. TRUSTe required all "members or licensees [to] disclose to users their information collection practices in exchange for the right to display a privacy seal on their Web site." Hertzel, *supra* note 69, at 445; *see also* FED. TRADE COMM'N, *supra* note 90, at 6.

[218] *See supra* note 195.

[219] *Cf.* Melanie A. Wakefield et al., *Use of Mass Media Campaigns to Change Health Behaviour*, 376 LANCET 1261 (2010) (describing successful state advertising about public health, including warnings about tobacco, fast food, and risky sexual behavior).

[220] *See Public Service Announcement*, *supra* note 199 (advising parents to take steps to protect their children's privacy).

[221] *See* Solove, *supra* note 88, at 1884.

[222] 16 C.F.R. §§ 312.3(b), 312.5 (2012).

[223] For a comprehensive review of the efficacy of notice and choice frameworks, see Reidenberg et al., *supra* note 204, at 489–97. For criticism on the efficacy of the notice and choice mechanism to regulate information privacy, see generally Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CALIF. L. REV. 1765 (2010).

[224] Users are "uninformed—or misinformed, as people rarely see, read, or understand privacy policies." Reidenberg et al., *supra* note 204, at 491.

[225] The notice and choice mechanism is considered impractical due to the amount of privacy policies online (which might also change from time to time), users' lack of knowledge of how third parties use data, users' inability to understand the effects of future aggregation of their data, and how users suffer from "bounded rationality and cognitive biases." *Id.* at 492–94 (quoting Ohm, *supra* note 201, at 931).

it creates undesirable externalities.[226] Generally, individuals make incorrect assumptions on how their privacy is protected and misconceive of how the data are used; many lack expertise in assessing the consequences of consent.[227]

If we accept consent as a proper form of regulation, policymakers must acknowledge that consent deals with IoToys insufficiently in its current form. Due to the potential risks of IoToys, regulators must require OSPs to do more than merely make "reasonable efforts" to obtain such consent.[228] Verification of parental consent must cross a higher threshold than that which COPPA currently sets. Methods of obtaining verifiable parental consent should necessitate parents actively calling or video-conferencing trained personnel who could assess if they understand the policy to which they are consenting.

Policymakers could also oblige companies to delimit choice of privacy preferences. They can set various restrictions on consent to data collection and retention, such as an obligatory opt-in mechanism, where by default, companies do not collect data from toys and do so only upon enabling such an option.[229] They could also reverse the choice and notice mechanism default so that consumers are obliged to signal their privacy preferences to the information collectors, not the reverse.[230] They could also oblige companies to offer consumers a choice between more costly services that protect their privacy and cheaper services that protect it less.[231]

3. *Data Minimization and Transparency*

COPPA currently requires data minimization through proportionality and necessity. It prohibits conditioning a child's online activity on the child's disclosure of more personal information than is reasonably necessary for participation in such activity.[232] While this requirement requires OSPs to collect

---

[226] The notice and choice mechanism potentially creates externalities because the disclosure of information by one individual could lead to disclosure of information of other individuals without their consent. *Id.* at 495.

[227] *See* Solove, *supra* note 88, at 1885–86.

[228] *Cf.* 15 U.S.C. § 6501(9) (2012) (describing the current requirements in the United States).

[229] *But see* Solove, *supra* note 88, at 1898–99 (describing the failure of opt-in consent).

[230] *See* Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 654 (2015).

[231] For example, AT&T offers that option to its customers. Jon Brodkin, *AT&T Charges $29 More for Gigabit Fiber That Doesn't Watch Your Web Browsing*, ARS TECHNICA (Feb. 16, 2015), https://arstechnica.com/information-technology/2015/02/att-charges-29-more-for-gigabit-fiber-that-doesnt-watch-your-web-browsing/ [https://perma.cc/GSM6-ZKBY]. This solution, however, has a social impact, as it implies that wealthy individuals deserve higher privacy protection than non-wealthy ones. Sophia Cope & Jeremy Gillula, Opinion, *AT&T Is Putting a Price on Privacy. That Is Outrageous*, THE GUARDIAN (Feb. 20, 2015), https://www.theguardian.com/commentisfree/2015/feb/20/att-price-on-privacy [https://perma.cc/WZ2S-CHJQ].

[232] 15 U.S.C § 6502(b)(1)(C) (2012); 16 C.F.R. §§ 312.3(d), 312.7 (2012).

only data that are necessary for the purposes for which they are collected, without proper transparency, it is extremely difficult to assess their datamining practices, data retention, and data transfers to third parties.

COPPA must be much more precise on data minimization. The use of vague language for keeping recordings on the merits of "data analysis purposes"[233] should not qualify as fulfilling this requirement. Policymakers must oblige companies to limit their data collection to what is required for the toy's core functions.[234] While defining core functions might not be easy, especially for IoToys devices that depend on advanced computational skills like machine learning, the default should still be set at no data collection unless these OSPs prove to the FTC that it is essential for the core functions of the toy.

Accordingly, policymakers should set limits on data retention and data sharing.[235] Even if OSPs allow parents to change the privacy settings of IoToys devices, on its own this would be insufficient to mitigate IoToys's risks.[236] Currently, COPPA requires that an OSP retain personal information "only as long as is reasonably necessary to fulfill the purpose for which the information was collected."[237] Policymakers must clarify this vague current requirement. OSPs must be obliged to clarify to consumers how long data is stored and when it will be deleted. As for data sharing, OSPs should not be allowed to share data with any third party unless the OSP proves that it has full control of how that data is used and an ability to delete it when necessary.

Clearly, ensuring that OSPs comply with the data minimization requirements necessitates some form of oversight. Transparently explaining the need for data use might not be easy. OSPs might have to disclose trade secrets, and even if they do not, they might not know beforehand what data will be needed in the future. These difficulties, however, do not completely rule out oversight measures. The obvious candidate to perform such oversight is the FTC; it could examine OSPs' practices, under secrecy if needed, and decide whether they comply with COPPA requirements. The Senate Committee on Commerce, Science, and Transportation actually suggested FTC monitoring of the connected toy space and exercising authority when appropriate.[238] This

---

[233] *See, e.g.*, TOYTALK, *Privacy*, *supra* note 54.

[234] *See* CHILDREN'S CONNECTED TOYS, *supra* note 57, at 2, 15; Emily McReynolds et al., Public Comment, Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys (Nov. 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/11/00038-141895.pdf [https://perma.cc/V2Q4-WMZW] (suggesting that toymakers limit how they collect and store data to allay parental privacy concerns).

[235] CHILDREN'S CONNECTED TOYS, *supra* note 57, at 2; McReynolds et al., *supra* note 234.

[236] Although a Senate committee report recommends for the FTC to advise parents to change the privacy settings of the toy to limit the amount of personal information that the toy collects and transmits and allow the toy to collect only information necessary for the toy to properly function, it might not be within the toy's options. *See* CHILDREN'S CONNECTED TOYS, *supra* note 57, at 2.

[237] 16 C.F.R. § 312.10 (2012).

[238] CHILDREN'S CONNECTED TOYS, *supra* note 57, at 16.

oversight, however, must also be implemented carefully, as it grants a state agent surveillance powers over individuals; as history shows, these powers can be misused by the state.[239] It would be wiser to invest a non-state data protection authority with such oversight powers.

4. *Toy and Information Security*

Properly securing the obtained data is naturally critical for safeguarding children's privacy. COPPA currently requires OSPs to maintain reasonable security policies.[240] The Senate Committee on Commerce, Science, and Transportation Office of Oversight and Investigations's advice to parents to strengthen their passwords and frequently update the toy's software,[241] while important, is still insufficient for data security. This requirement must be clarified and recalibrated, as it does not greatly advance IoToys's security levels.

Prior to such recommendations, one may at least presume that legal intervention might not be needed when market players possess high incentives to secure their products and services.[242] Arguably, low security measures and data breaches could result in damage to toymakers' reputations and monetary losses from fines, lawsuits, or simply losing customers. The state, in fact, encourages parents to respond actively to IoToys's security measures. The Senate Committee on Commerce, Science, and Transportation Office of Oversight and Investigations advises parents to examine companies' prior history of security breaches.[243] The FBI has further recommended that parents examine "the toy's Internet and device connection security measures" and probe "any known reported security issues," "use toys in environments with trusted and secured Wi-Fi Internet access," "[r]esearch where user data is stored . . . and whether any publicly available reporting exists on their reputation and [stance on] cyber security," and "[e]nsure the toy is turned off . . . when not in use."[244]

Prima facie, IoToys manufacturers and OSPs would wish to invest in measures to protect their products, services, reputation, share price, and customers from harm. As this market-based approach suggests, with proper incentives, the modality of law is not needed—absent substantial market failures

---

[239] For more on surveillance in the digital age, see generally BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015); Niva Elkin-Koren & Eldar Haber, G*overnance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105 (2016).

[240] 16 C.F.R. §§ 312.3(e), 312.8 (2012).

[241] CHILDREN'S CONNECTED TOYS, *supra* note 57, at 2, 16.

[242] This assumption is often attributed to Adam Smith's coining of the "invisible hand," i.e., that market players acting in their own self-interest will react to demand, which reflects the preferences of members of society and thus promotes the social good. *See* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS (Sálvio Marcelo Soares ed., 4th ed. 2007) (1776).

[243] *See* CHILDREN'S CONNECTED TOYS, *supra* note 57, at 2, 15 (recommending FTC advice to parents).

[244] FED. BUREAU OF INVESTIGATION, *supra* note 199.

that would prevent the market from reaching its anticipated equilibrium point. But as shown next, while the market as a modality to regulate cybersecurity could be an important component of any solution,[245] it is insufficient on its own to regulate IoToys properly due to the existence of market failures.

First, the market-based approach's reliance on consumers' discontent with security measures is due to failures. It presumes no cognitive failures, no information gaps, and the presence of expertise to evaluate security measures properly. Even if the state adds regulatory requirements of disclosure like security standards or data breach notifications[246] to reduce information gaps—commonly termed the *regulation through disclosure* approach[247]—this will not necessarily lead to a market response.[248] It might be too vague for consumers to fully understand because of the aforementioned cognitive biases or simply not be fully comprehensible without substantial expertise in cybersecurity.

In addition, consumers may lack the ability to indicate their discontent with cybersecurity measures in the IoToys market as it is not fully competitive. This market currently operates with limited competition—controlled by key market players like Mattel and ToyTalk. Their products and services are not necessarily similar to their competitors', hence are not fully substitutive. From a child's perspective, it is fairly intuitive that not all children will view Hello Barbie as equivalent to Cayla. So without a fully competitive market it is difficult to assume that consumers could markedly alter these companies' security policies.[249] Notably, however, IoToys devices are certainly not a necessity, and parents' discontent could be realized simply by their not purchasing any IoToys device.

As the market in itself will be insufficient to promote optimal cybersecurity measures, legal intervention is most likely required. Recalibration of COPPA must begin by expanding beyond maintaining reasonable procedures to protect the confidentiality, security and integrity of personal information collected from

---

[245] Professor Lawrence Lessig suggested four modalities that could regulate behavior: market, social norms, technology (code), and law. LAWRENCE LESSIG, CODE: VERSION 2.0 120–37 (2006); *see also* LAWRENCE LESSIG, FREE CULTURE 116–73 (2004).

[246] Data breach notifications statues in the United States are currently state legislated and usually require private and government entities to notify individuals of security breaches of information involving personally identifiable information with notable exceptions like encrypted data. *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 297 (2014).

[247] Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 613 (1999).

[248] *See, e.g.*, Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256, 280–81 (2011) (concluding that data breach disclosure laws' efficacy is lower because consumers do not respond to them by taking any action). For more on data breach notification regulation, see Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007).

[249] *See, e.g.*, Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1517 (2013) ("[S]trategically significant firms in uncompetitive markets are less likely to adequately invest in cyber-security than ordinary firms in competitive markets.").

children. Policymakers must set a higher threshold than "reasonable" and demand that toy manufacturers and OSPs comply with high security standards for the IoToys device and the stored data. They must establish security standards that OSPs and third parties must meet to be able to collect and retain data. These measures must also address the threat of real-time interception of data, not merely its collection and storage. OSPs must be obliged to use cutting-edge security measures that will stop—or at least substantially reduce—the possibility of hacking the toy and the stored data.

Inter alia, these measures might include requirements to meet predetermined security standards, conduct security audits, implement bug bounty programs,[250] use strong encryption standards, and actively update security measures.[251] The Senate Committee on Commerce, Science, and Transportation Office of Oversight and Investigations has in fact suggested that toymakers build in effective security from the start.[252] These suggestions should become obligatory, but also be further clarified. Policymakers must clarify exactly what robust security means and make sure that companies are subjected to periodic external audits as part of the suggested oversight. Beyond the use of strong encryption, they should incentivize toymakers to implement anonymization measures,[253] differential privacy,[254] and any other PET tools,[255] as long as the FTC can verify their applicability to safeguarding children's privacy.

---

[250] ToyTalk, for instance, currently "offers a monetary bounty for reports of qualifying security vulnerabilities." *See PullString: Bug Bounty Program,* HACKERONE, https://hackerone.com/toytalk [on file with the *Ohio State Law Journal*] (last updated Apr. 26, 2018).

[251] *See* KIDS & THE CONNECTED HOME, *supra* note 4, at 15; CHILDREN'S CONNECTED TOYS, *supra* note 57, at 2.

[252] *See* CHILDREN'S CONNECTED TOYS, *supra* note 57, at 15.

[253] Realizing that speech recognition must obtain large quantities of data to improve, regulators could allow data collection and retention only when children are not linked with the data after its processing. That would mean that the data could still exist, but linking it to a specific user would be highly difficult. Notably, at least one IoToys OSP declares that it anonymizes the data and further ensures it is stored in multiple different places. *See* Sara Sorcher, *The Internet of Toys Raises New Privacy and Security Concerns for Families*, CHRISTIAN SCI. MONITOR: PASSCODE (July 22, 2016), https://www.csmonitor.com/World/Passcode/2016/0722/The-Internet-of-Toys-raises-new-privacy-and-security-concerns-for-families [https://perma.cc/AZY4-QU22] (reporting that Elemental Path, which makes a talking dinosaur toy, says it works to anonymize data, while other companies do not).

[254] Differential privacy relates to a method by which noise is added systematically to results of data queries so "no single person's inclusion or exclusion from the database can significantly affect the results of queries." Jane Bambauer et al., *Fool's Gold: An Illustrated Critique of Differential Privacy*, 16 VAND. J. ENT. & TECH. L. 701, 703 (2014). Using differential privacy correctly should assure that no user could infer anything about another user. *Id.* For an analysis and critique of differential privacy, see *id.*

[255] *See, e.g.*, *Platform for Privacy Preferences (P3P) Project*, *supra* note 174 (detailing a PET that allows companies to "express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents").

5. *Effective Enforcement*

The FTC's option to sanction COPPA violations is in itself insufficient to be considered effective enforcement.[256] The FTC must be more involved in *ex ante* and *ex post* enforcement practices. From an *ex ante* perspective, the FTC must closely oversee the implementation of privacy policies in practice, and not merely rely on OSPs' statements. This became evident with the data breach of VTech: the FTC learned *ex post* that the company did not comply with its own privacy policy, which falsely stated that it used encryption when in fact it did not encrypt any information.[257] Even without adhering to direct oversight, at the very least the FTC must investigate and rectify instances where reporters show that an IoToys device is not secure enough.[258] They must use reliable mechanisms to provide substantial sanctions against noncompliance with regulations or simply not approve marketing or sale on the grounds of children's safety.[259]

These measures must be complemented with *ex post* measures such as imposing steep fines as a potential deterrent. True, the effect of deterrence might be disputable in general;[260] nonetheless, the FTC should exercise its vested powers of enforcement to impose the highest fines possible.[261] Sanctioning companies like VTech to the tune of $650,000[262] for a substantive data breach is unlikely to advance the deterrence rationale, considering its $689.4 million gross profits in 2017.[263] OSPs must not see fines as costs of doing business and

---

[256] The FTC acknowledged this ability to effectively enforce COPPA as a critical component to protecting privacy online. *See* FED. TRADE COMM'N, *supra* note 90, at i.

[257] *See* Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act, *supra* note 163.

[258] Research showed that there is a high rate of potential COPPA violations in apps that are directed to children, while pointing to troubling lack of oversight. *See* Serge Egelman, *We Tested Apps for Children. Half Failed to Protect Their Data*, WASH. POST: SWITCH (July 27, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/07/27/we-tested-apps-for-children-half-failed-to-protect-their-data [https://perma.cc/4APB-2TKX]; *see also supra* notes 161–162.

[259] *See* Natasha Lomas, *Call to Ban Sale of IoT Toys with Proven Security Flaws*, TECHCRUNCH (Nov. 15, 2017), https://techcrunch.com/2017/11/15/call-to-ban-sale-of-iot-toys-with-proven-security-flaws [https://perma.cc/7M7R-KKFM] (explaining the vulnerability of children's data and the ease of obtaining data from IoT toys, calling for security to be "an absolute priority").

[260] Generally speaking, deterrence theory has been criticized over the years. *See, e.g.*, Dan M. Kahan, *The Theory of Value Dilemma: A Critique of the Economic Analysis of Criminal Law*, 1 OHIO ST. J. CRIM. L. 643, 643–47 (2004).

[261] The FTC fines are often quite low in relation to the gravity of the violations and the overall net profit of the violators. Nevertheless, COPPA violations sometimes draw rather large fines, ranging from $250,000 to $3,000,000. Solove & Hartzog, *supra* note 83, at 605, 647.

[262] *See* Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act, *supra* note 163.

[263] *See Annual Report 2017*, VTECH HOLDING LTD., 6 (2007), https://www.vtech.com/

should reflect further on the gravity of poor security measures. Policymakers should thus implant in the FTC more substantial regulatory teeth. This would enable the Commission's fines not merely to reflect the level of consumer loss but rather to sanction violations, with fines as percentages of annual global turnover.[264] If the FTC continues to act as a data protection authority, policymakers must further invest in and expand the purview of the Division of Privacy and Identity Protection—the body devoted to privacy issues—to issuing high fines and conducting meaningful oversight of OSP practices.[265]

Legal intervention is thus greatly needed to better secure informational privacy of children in the IoToys market. COPPA regulation must frequently be updated to better address the risks that IoToys entails, and frequently revisited in view of technological changes that could affect the risks in these toys. For example, the future IoToys market might expand the current children-to-toy interaction to children-to-children. If, for instance, Hello Barbies begin exchanging information, children might also be exposed to harassment in the form of cyberbullying, along with further dangers to their privacy.[266]

All in all, COPPA should become more oriented to the privacy risks of IoToys, and policymakers must not presume that the potential risks to children's privacy from being online do not change over time. Children's privacy must be taken more seriously, and the ways technological developments could negatively affect it must be acknowledged. If an IoToys device increases the risks to children's privacy, parents must also become more involved in safeguarding their children.[267] Their involvement, however, should not be treated lightly, as it bears on important normative questions that must be further addressed: what are the implications of the tradeoff between children's security and children's privacy—or stated differently—between parents' empowerment and children's protection?[268] More particularly, should children's right to privacy be viewed only as a right from third-parties or also from their parents?[269] In other words, how can we ensure children's privacy outside their

---

wp-content/uploads/2017/06/AR2017_eng.pdf [https://perma.cc/MD7T-ZHPU].

[264] This approach was recently chosen by the European Union in its General Data Protection Regulation (GDPR). *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, Art. 83, 2016 O.J. (L 119) 1.

[265] *See* Solove & Hartzog, *supra* note 83, at 600–01 (noting that the FTC's staff devoted to privacy issues is relatively small).

[266] *See* Kay Mathiesen, *The Internet, Children, and Privacy: The Case Against Parental Monitoring*, 15 ETHICS & INFO. TECH. 263, 263 (2013) (describing children's privacy risks on the internet).

[267] McReynolds et al., *supra* note 234.

[268] *See* Milda Macenaite, *From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation*, 19 NEW MEDIA & SOC'Y 765, 766 (2017) (discussing the "empowerment versus protection" dilemma in child rights debates).

[269] *See id.*

household but also not completely abolish it within what they view as their safe place?

V. TAKING CHILDREN'S PRIVACY SERIOUSLY

Parents have the responsibility to safeguard their offspring from dangers. They must make decisions regarding various aspects of their children's lives, especially their health, development, and safety. To do so, parents might oblige children, inter alia, to "play in rubber-cushioned playgrounds, use sanitizing gel, sit in car seats, and wear helmets and kneepads while riding their bicycles."[270] They might also become closely involved in their lives and even use sensors and monitors to assure their safety.[271] While parents might always have been involved in their children's lives to some extent, researchers have witnessed an increase in parents' involvement since the mid-1980s. To date, it has developed into a phenomenon dubbed helicopter parenting, smothering mothering, or child-centered parenting, among other proposed names.[272] Essentially, children today are probably "the most watched over generation" in history.[273]

The notion that parents nowadays should be more protective could be important and perhaps challenged—but nonetheless beyond the scope of this Article. The purpose of this part is rather modest. It seeks to identify how the regulatory framework that governs IoToys subjects children to this form of parenting and even takes it a step farther than the regulation of online activities through websites. It discusses the tension between children's protective rights, like the right to be safeguarded from harms, and their participatory rights to make decisions.[274] It also further seeks to discuss the *privacy protection paradox*,[275] namely that children's privacy cannot be safeguarded properly when parents obtain tools—that IoToys makers are encouraged to provide—to constantly spy on them, when the rationale behind such tools is outside the regulatory framework.

---

[270] Gaia Bernstein & Zvi Triger, *Over-Parenting*, 44 U.C. DAVIS L. REV. 1221, 1233 (2011).

[271] *Id.*

[272] This phenomenon generally describes parents that are "obsessed with their children's success and safety [and] vigilantly hover over them, sheltering them from mistakes, disappointment, or risks." Kathleen Vinson, *Hovering Too Close: The Ramifications of Helicopter Parenting in Higher Education*, 29 GA. ST. U. L. REV. 423, 424–25 (2013). It had also been characterized, inter alia, as "'invasive parenting', 'overparenting,' 'aggressive parenting,' 'modem parenting,' and 'snowplow parenting.'" *Id.* at 424 n.4 (citing Nancy Gibbs, *The Growing Backlash Against Overparenting*, TIME (Nov. 20, 2009)); Bernstein & Triger, *supra* note 270, at 1225; Lisa Belkin, *Let the Kid Be*, N.Y. TIMES MAG. (May 29, 2009), https://www.nytimes.com/2009/05/31/magazine/31wwln-lede-t.html [https://perma.cc/EYX4-SY6R].

[273] *See* NEIL HOWE & WILLIAM STRAUSS, MILLENNIALS RISING 9 (2000) (arguing that the millennials' generation is "the most watched over generation in memory").

[274] *See* Macenaite, *supra* note 268, at 766–67.

[275] *See* THE PROTECTION OF CHILDREN ONLINE, *supra* note 49, at 37.

A. *Parenting in the IoToys Era*

Parenting generally involves a balance of risk management.[276] Many parents might view good or responsible parenting as being all-knowing, which requires them to monitor their children's behavior.[277] They might monitor their children even before birth, using ultrasound screening to detect fetal anomalies, see their unborn baby's movements, and hear its sounds.[278] After birth, parents will often monitor their children's behavior and development directly, by watching and listening to them, or indirectly, by means of technology, such as wearable devices and various types of sensors and monitors.[279] Parents might even monitor their children when another caregiver is present by using, inter alia, cameras hidden inside another object ("nanny cams").[280] When their children are old enough to interact with the digital world, parents might monitor their conduct by various methods. Parents' consent to their children using the internet, for instance, might require imposing rules and restrictions such as placing the computer in a shared space[281] or obliging their children to share the content of their conversations and even their usernames and passwords.[282] Parents might also embrace social approaches, like by educating children to share what they are doing or by using technical tools like monitoring software.[283] Essentially, many parents will attempt to strengthen their control and track almost everything their children do offline and online.[284]

It is generally uncontested that keeping an eye on children, especially young ones, is extremely important at any time, let alone in the digital age.[285] Parents might fear that their children's data will be misused and might also be alert to

---

[276] *See* David Pimentel, *Criminal Child Neglect and the "Free Range Kid": Is Overprotective Parenting the New Standard of Care?*, 2012 UTAH L. REV. 947, 961–63 (2012).

[277] *See* DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 70–72 (2014) (ebook).

[278] *See* Bernstein & Triger, *supra* note 270, at 1232; Deborah Lupton & Ben Williamson, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, 19 NEW MEDIA & SOC'Y 780, 783 (2017).

[279] Bernstein & Triger, *supra* note 269, at 1232–33; Lupton & Williamson, *supra* note 276, at 783–84. *See generally* Margaret K. Nelson, *Watching Children: Describing the Use of Baby Monitors on Epinions.com*, 29 J. FAM. ISSUES 516 (2008) (discussing parents' responses to anxiety about their children through reviews of baby monitors).

[280] *See 5 Great Nanny Cams to Install If You Want to Check in on Your Children*, FATHERLY (Dec. 18, 2018), https://www.fatherly.com/gear/best-nanny-cams/ [https://perma.cc/D6HC-RUMA]; Lupton & Williamson, *supra* note 278, at 783–84 (noting "[i]ntimate surveillance" of infants and children and camera surveillance in schools).

[281] *See* BOYD, *supra* note 277, at 72–73.

[282] *Id.* at 72–73.

[283] *See* Jos de Haan, *Maximising Opportunities and Minimising Risks for Children Online*, *in* KIDS ONLINE: OPPORTUNITIES AND RISKS FOR CHILDREN 187, 192 (Sonia Livingstone & Leslie Haddon eds., 2009).

[284] *See* BOYD, *supra* note 277, at 70–74.

[285] Warmund, *supra* note 101, at 190.

their exposure to harmful content, cyberbullying, and inappropriate contact.[286] These fears might be further enhanced by perceiving their children's interactions as less visible to them online than in the kinetic world.[287] Under this assumption, parents will use technology to monitor their children online as a responsive measure against the risks of technology.[288]

While parents' mediation is effective in reducing online risks to their children is disputable,[289] these fears are real, and children's safety should be on the agenda of any parent. As discussed throughout this Article, IoToys could clearly expose children to various risks, and parents might wish to intensify control over their children's play because of these risks and the invisibility of their actions from their point of view. COPPA regulation deals directly with protecting children's privacy from third parties misusing their data. With the privacy risks of the internet in mind, American regulators obliged OSPs to provide a right of parental review, which includes granting parents the right to review the collected information.[290]

Some OSPs took the right of parental review a step further in IoToys, by providing parents real-time access to their children's recordings.[291] In some instances they could even be notified when a new recording was made.[292] At first sight, this move seems to strengthen parents' control in the IoToys context, and therefore should be encouraged, as it acknowledges the potential risks to the sensitive information that children might convey to third parties. The FBI even publicly recommended that parents closely monitor their children's activity with the toys.[293] However, this form of monitoring is troubling from a privacy perspective.

While COPPA regulation supposedly increases children's privacy by strengthening parents' control over the disclosure of sensitive information, it might further jeopardize children's privacy from a different perspective: the children's. Due to the characteristics of many IoToys devices, children might become convinced that the IoToys device is their best friend—even anthropomorphize it—and consequently share their deepest secrets with it.[294] Perhaps obviously, the regulatory framework does not deem such secrets

---

[286] *See generally* Mathiesen, *supra* note 266 (discussing cyberbullying and harmful content).

[287] *See id.* at 266.

[288] *Id.* at 267.

[289] For an empirical work on reducing online risks by parental mediation, see generally Sonia Livingstone & Ellen J. Helsper, *Parental Mediation of Children's Internet Use*, 52 J. BROADCAST ELECTRONIC MEDIA 581 (2008).

[290] 15 U.S.C. § 6502(b)(1) (2012); 16 C.F.R. § 312.6(a)(3) (2012).

[291] *See* TOYTALK, *Privacy*, *supra* note 54 ("You may review and delete voice recordings that are in your parent account via the Settings page when you log in to ToyTalk's website. To review or delete such voice recordings, click on the 'Conversation Link.'").

[292] *Id.* ("We may periodically contact parents to inform them when a voice recording is available under their account.").

[293] FED. BUREAU OF INVESTIGATION, *supra* note 199.

[294] *See supra* Part 0.

sensitive information per se, as safeguarding this information from third parties might not seem important. OSPs that sometimes make it easy for parents to share IoToys devices' recordings through social media like Facebook, YouTube, and Twitter further demonstrate the secrets' proclaimed non-sensitive nature.[295] From the children's perspective, however, their secrets are probably the most valuable privacy rights they own.[296]

Children's view of privacy will probably not change how policymakers conceive personal information. It should not, however, promote parental monitoring when such behavior could further risk children's conception of privacy. The main rationale behind COPPA was not to foster parental surveillance of their children online but to aid parents who wanted their children to take advantage of the internet, while obtaining better control of the practices of the websites they visited and the information requested from them.[297] IoToys essentially could become a powerful surveillance device for parents, who could now extract all their children's secrets without their knowledge or consent. It designates parents as surveillance officers and normalizes such conduct for both parents and their children—when they become aware of it in the future. It further illustrates important normative questions in the realm of children's privacy that are usually less discussed in the literature: What are the implications of constantly monitoring children's privacy? Should children possess the right to privacy from their parents? Children lack autonomy over most aspects of their lives, so why should IoToys differ?

B. *Child Development and Privacy*

While monitoring children's play in IoToys could be important in lessening the privacy risks they entail, ubiquitous parental surveillance carries potentially negative consequences closely linked to their development and well-being. At early stages of life like infanthood, this might be less evident, as children lack a "theory of mind"; namely, they are unable to distinguish self from other.[298] After that stage at approximately age four, children learn that they can keep secrets from their parents.[299] That is when the potentially negative effect of ubiquitous surveillance begins.

---

[295] *See* TOYTALK, *Privacy*, *supra* note 54.

[296] *See infra* Part III.A.

[297] It is notable that COPPA was partially designed to enhance parental involvement in a child's online activities. This, however, is not the rationale behind COPPA per se, but rather a tool for parents to achieve the goals of COPPA, i.e., to help protect the safety of children, maintain the security of children's personal information collected online, and limit the collection of personal information from children without parental consent. *See* 144 CONG. REC. 23,926 (1998) (statement of Sen. Bryan).

[298] *See* David Premack & Guy Woodruff, *Does the Chimpanzee Have a Theory of Mind?*, 1 BEHAV. & BRAIN SCI. 515, 515 (1978).

[299] Beate Sodian et al., *Early Deception and the Child's Theory of Mind: False Trails and Genuine Markers*, 62 CHILD DEV. 468, 479 (1991). *See generally* Malinda J. Colwell et al., *Secret Keepers: Children's Theory of Mind and Their Conception of Secrecy*, 186 EARLY

The world's perception of children has been the subject of many scholarly debates, from Jean Piaget's development stages and process[300] to Donald Winnicott's monumental work on stages of child development and practice of childhood play.[301] A key example is Erik Erikson's work, which stresses the importance of the years from middle childhood (approximately ages six to ten) to early adolescence (approximately ages eleven to fourteen) for children's development.[302] Erikson argued, inter alia, that these stages are important for developing a sense of self-esteem and individuality.[303] Within these psychological assessments, play itself is also is an important part of how children learn about the world, and parents' intrusion could impede their learning.[304] Control over personal information is also crucial for children's development, as its absence could affect the adolescent's dignity and personhood and the development of intimate relationships.[305] Especially regarding IoToys, acknowledging the psychological importance of keeping secrets should not be easily dismissed.

Regardless of IoToys, one might argue that it is within the parents' prerogative to determine the extent to which they protect their children's privacy. Parents, for instance, could limit their children's privacy in various ways, such as intruding in their personal space; knowing their personal interactions and associations, such as where and with whom they meet; and even requiring them to share their daily activities or their hopes, dreams, and fears.[306] Arguably, the perceived risks of the digital world do not change the scope of

---

CHILD DEV. & CARE 369 (2016) (associating the theory of mind, a child's understanding of secrets, and a child's self-regulation); *see also* Heinz Wimmer & Josef Perner, *Beliefs About Beliefs: Representation and Constraining Function of Wrong Beliefs in Young Children's Understanding of Deception*, 13 COGNITION 103, 124 (1983) (finding that between ages four and six, a child develops the ability to "represent wrong beliefs").

300 JEAN PIAGET, THE CHILD'S CONCEPTION OF THE WORLD (1926).

301 D.W. WINNICOTT, THE CHILD AND THE FAMILY (1957); D.W. WINNICOTT, THE CHILD, THE FAMILY AND THE OUTSIDE WORLD (1964); D.W. WINNICOTT, THE FAMILY AND INDIVIDUAL DEVELOPMENT (1965). For an excellent summary of children's perception of the right to privacy, see generally Sunny Kalev, "אני מחליט עליי" — פרטיות של ילדים בעידן הדיגיטלי והזכות לחזרה מהסכמה הורית [*"I Decide for Myself" – Children's Privacy in the Digital Age and the Right to Withdraw from Parental Consent*], 41 TEL AVIV U. L. REV. 61 (2018).

302 ERIK H. ERIKSON, CHILDHOOD AND SOCIETY (2d ed. 1963).

303 *Id.*; *see also* Jacquelynne S. Eccles, *The Development of Children Ages 6 to 14*, 9 FUTURE CHILD. 30, 32–34 (1999).

304 *See* Emmeline Taylor & Katina Michael, *Smart Toys That Are the Stuff of Nightmares*, 35 IEEE TECH. & SOC'Y MAG. 8, 9 (2016).

305 *See* Gary B. Melton, *Minors and Privacy: Are Legal and Psychological Concepts Compatible?*, 62 NEB. L. REV. 455, 488–89 (1983).

306 *Id.* at 488.

this prerogative, they indeed even intensify this need.[307] By this approach, parents must be in greater control, especially in the digital world.[308]

From a legal perspective, parents are not normally prohibited from recording their children or even reading their secret diaries.[309] Parents' fundamental right to make decisions regarding the "care, custody, and control of their children"[310] is even protected by the Due Process Clause of the Fourteenth Amendment.[311] Parents decide what is best for their children and whether to tell their children that parents can access their children's conversations. Under some circumstances, parents could even be immune to tort liability under the parental immunity doctrine.[312] As a result, children do not possess the right to conceal information from their parents.[313] COPPA regulation is troubling not because parents are generally entitled to spy on their children but because the regulatory framework encourages OSPs to furnish such measures.[314] When parents buy their children an IoToys doll that is supposedly their children's new best friend, the children may not suspect that their parents can eavesdrop on every conversation they have with the doll.[315]

Equally troubling is that parents' depriving their children of privacy is becoming more invisible to their children than ever. Children are usually well aware of their parents' control over their personal space. For instance, if parents decide that their children should not have privacy in their room, the children see at once that there is no door, and this might affect their behavior.[316] They might

---

[307] *See* Antigone Davis, *Hard Questions: So Your Kids Are Online, but Will They Be Alright?*, FACEBOOK NEWSROOM (Dec. 4, 2017), https://newsroom.fb.com/news/2017/12/hard-questions-kids-online [https://perma.cc/H8VT-UXVZ].

[308] *Id.* ("[P]arents want to know they're in control. They want a level of control over their kids' digital world that is similar to the level they have in the real world.").

[309] *See* Mathiesen, *supra* note 266, at 264.

[310] Francis Barry McCarthy, *The Confused Constitutional Status and Meaning of Parental Rights*, 22 GA. L. REV. 975, 976 (1988) (internal citation omitted).

[311] *See* U.S. CONST. amend. XIV § 1. For the Supreme Court ruling on parents' discretion over their own children, see *Troxel v. Granville*, 530 U.S. 57, 78 (2000). For further information on the history of parental autonomy in common law jurisdictions, see McCarthy, *supra* note 310, at 975–84.

[312] Under the parental immunity doctrine, children were unable to sue their parents for tort claims. For more on the demise of the parental immunity doctrine, see, for example, David Pimentel, *Fearing the Bogeyman: How the Legal System's Overreaction to Perceived Danger Threatens Families and Children*, 42 PEPP. L. REV. 235, 241–42 (2015); Pimentel, *supra* note 276, at 954–55. For a discussion on children's rights to sue their parents in the context in tort for their child's injury, see, for example, Maureen S. Binetti, *The Child's Right to "Life, Liberty and the Pursuit of Happiness": Suits by Children Against Parents for Abuse, Neglect, and Abandonment*, 34 RUTGERS L. REV. 154, 156–57 (1981).

[313] Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759, 780 (2011).

[314] COPPA Rule, *supra* note 82.

[315] McReynolds et al., *supra* note 234, at 2.

[316] A fairly known example of behavioral shaping by surveillance is the toy based on the Christmas book *Elf on the Shelf*. Alex Steed, *No to 'Elf on the Shelf': Christmas Shouldn't*

then seek ways to compensate for their privacy loss by a variety of methods, like keeping a secret journal. The interpretation of COPPA regulation in the realm of IoToys effectively ends the children's privacy boundary management by making interference invisible to them. It tricks them into believing that they can manage their privacy boundaries, while their parents constantly betray their trust.

Such a form of invisible monitoring could have dire consequences for children's trust and development and could also further shape their conception of privacy. One might argue that data collection and various forms of monitoring are mostly invisible to adults too, and perhaps these mechanisms actually better prepare children for the "real world."[317] This notion augments a well-known idiom about the demise of privacy in the digital age.[318] This Article, however, posits differently. Privacy still matters, perhaps even more in the digital era. That children use the digital world does not imply that they do not care about their privacy.[319] They simply view it differently from adults.[320] For instance, children could view privacy simply as "aloneness,"[321] "to hide secrets or special

---

Be an Extension of Our Surveillance Culture, BANGOR DAILY NEWS (Dec. 5, 2014), http://bangordailynews.com/2014/12/05/opinion/contributors/no-to-elf-on-the-shelf-christmas-shouldnt-be-an-extension-of-our-surveillance-culture [https://perma.cc/M34Y-WFQT]. In the book, Carol Aebersold and Chanda Bell describe a minion of Santa who spies on children. *Id.* Based on the book, an "Elf on the Shelf" doll was sold to parents to teach children to alter their behavior when been "watched" by the elf. *Id.* For more on the privacy implications of the *Elf on the Shelf*, see Laura Elizabeth Pinto & Selena Nemorin, *Normalizing Panoptic Surveillance Among Children: The Elf on the Shelf*, 24 OUR SCHOOLS/OUR SELVES 53, 57–59 (2015).

[317] For more on the invisibility of data collection and privacy, see Saadi Lahlou et al., *Privacy and Trust Issues with Invisible Computers*, 48 COMM. ACM 59, 59–60 (2005).

[318] Many argue that privacy is dead or at least that it deserves minimal protection at best in the digital age, and that even if privacy still exists it is merely a tradeable currency. *See, e.g.*, Polly Sprenger, *Sun on Privacy: 'Get over It,'* WIRED (Jan. 26, 1999), https://www.wired.com/1999/01/sun-on-privacy-get-over-it [https://perma.cc/QPJ5-2R9H]. Scott McNealy, chief executive officer of Sun Microsystems, is famously quoted stating "You have zero privacy anyway. . . . Get over it." *Id.; see also* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1462–63 (2000) (suggesting that the collection of information is a means of gathering power and that the law should protect information privacy). For more on the privacy-as-currency argument, see James P. Nehf, *Shopping for Privacy Online: Consumer Decision Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 14–17 (2005).

[319] *See generally* BOYD, *supra* note 277, at 54–55 ("Social media has introduced a new dimension to the well-worn fights over private space and personal expression.").

[320] *See, e.g.*, Sonia Livingstone, *Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family*, *in* COMPUTERS, PHONES, AND THE INTERNET: DOMESTICATING INFORMATION TECHNOLOGY 130, 132 (Robert Kraut et al., 2006) ("Children seek privacy, but as a means to an end not an end in itself.").

[321] *See* Melton, *supra* note 305, at 488. They might also view privacy as "being alone, managing information, being unbothered, and controlling access to places." Maxine Wolfe, *Childhood and Privacy*, *in* CHILDREN AND THE ENVIRONMENT 175, 190–96 (Irwin Altman & Joachin F. Wohlwill eds., 1978) (surveying children's definitions of privacy).

things," "to keep things to yourself," or "not to talk to strangers."[322] They might value privacy as an enabler tool "to engage in identity play, seek advice, form relationships, and immerse themselves in peer communication."[323] When children experience constant surveillance by their parents, it shapes their understanding of privacy and limits their ability to make independent choices.[324] Surveillance becomes even more important when their lives are already largely monitored by their parents,[325] and further strengthens the traditional power structure of the "all-knowing" adult over the "all-learning" child.[326]

Parents should be generally aware of what their children do with IoToys devices, but this should also be balanced properly by the child's right to privacy.[327] Their privacy rights—including from their parents—should not be easily discarded. Parents must take into account how these practices could affect their child's well-being. Certainly, most children will not be able to comprehend the privacy risks of IoToys, as they are too abstract. Children might not even care if OSPs mine their data or use it for various purposes. This is why parents are tasked to consent on their child's behalf. But being unaware that IoToys devices record their conversations[328] and that their parents have access to them, might change children's attitudes toward their parents upon discovering the monitoring and the meaning of privacy.[329]

To clarify, this Article does not pretend to prefer one form of parenting over another. Perhaps personal safety almost always triumphs over privacy, in which case parental autonomy should be almost absolute. If parents wish to constantly monitor their children's behavior, with proper analysis of the tradeoff between their safety and their well-being, perhaps they should be allowed to. On the other hand, the constitutional right to parental autonomy is not absolute. Even today, along with cracks in the parental immunity doctrine, parents' privilege to raise children as they see fit could sometimes be challenged when child protection

---

[322] *See* Leah Zhang-Kennedy et al., *From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats*, IDC '16 PROC. 15TH INT'L CONF. ON INTERACTION DESIGN & CHILD. 388, 392 (2016).

[323] Priya Kumar et al., *'No Telling Passcodes out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online*, 1 PACM ON HUM.-COMPUTER INTERACTION 64, 64:2 (2017); Livingstone, *supra* note 320, at 152.

[324] *See* BOYD, *supra* note 277, at 74.

[325] *Id.* at 76 ("Privacy is especially important for those who are marginalized or lack privilege within society.").

[326] *See* Allison Druin, *The Role of Children in the Design of New Technology*, 21 BEHAV. INFO. TECH. 1, 1 (2002).

[327] *See* de Haan, *supra* note 283, at 193 ("Parents should be broadly aware of what their children do online, although this should be balanced by the child's right to privacy."). For an analysis on why children should have a right to privacy, see Mathiesen, *supra* note 266, at 269–72.

[328] McReynolds et al., *supra* note 234, at 2.

[329] Meg Leta Jones & Kevin Meurer, *Can (and Should) Hello Barbie Keep a Secret?*, IEEE ETHICS (2016), https://ssrn.com/abstract=2768507 [https://perma.cc/5EUL-D526].

and safety concerns arise.[330] The state could in fact triumph over parental autonomy under some circumstances by regulating the parent–child relationship.[331] Accordingly, children's privacy rights should be treated as part of their welfare and thus not be easily waivable by their parents as a default.[332]

At the very least, COPPA should not promote such potentially deceptive practices without the child's involvement in the process. If designed to safeguard children's privacy, COPPA must not further foster violating that privacy by granting parents better tools to do so. It must not designate parents as surveillance officers. Policymakers should further address the parent–child dimension within the notions of notice and consent. By doing so, they can make children part of the solution to the risks of the digital era rather than reinforce an existing problem.

C. *Children's Choice?*

Accepting the potential arguments against this form of parental mediation does not necessarily lead to regulating IoToys. The sanctity of the family unit is important, and interference should be generally limited.[333] Even if delicate regulation takes place, COPPA might not be the right tool for it. Still, regulators should at least acknowledge children's privacy interests, in contrast to the concept of privacy as portrayed by parents. Not only does COPPA disregard children's view of privacy, it indeed enhances the violation of that privacy, as children perceive it. It takes away children's freedom to decide what to disclose to their parents, as it promotes their full access to stored content. Essentially, COPPA fails to internalize the complexity of the child–parent relationship.[334]

Promoting the use of sophisticated spying devices for parents to discover their children's secrets is not among the values embedded in COPPA regulation and should therefore be minimized through other factors. The parent–child relationship should not be set aside, and children's trust in their parents should

---

330 *See, e.g.*, Elizabeth G. Porter, *Tort Liability in the Age of the Helicopter Parent*, 64 ALA. L. REV. 533, 557, 559–60, 573–75 (2013).

331 *See* Elaine M. Chiu, *The Culture Differential in Parental Autonomy*, 41 U.C. DAVIS L. REV. 1773, 1786–90 (2008).

332 For an argument that privacy is not always a waivable right, see JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 148 (2012).

333 *See* The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2012) (instituting federal law that protects the privacy of student educational records and allows parents the right to "inspect and review" them).

334 The parent-child relationship is frequently discussed in academic literature in various contexts. For a discussion of this relationship complexity, see, for example, Katharine T. Bartlett, *Re-Expressing Parenthood*, 98 YALE L.J. 293, 326 (1988); Janet L. Dolgin, *The Fate of Childhood: Legal Models of Children and the Parent-Child Relationship*, 61 ALB. L. REV. 345, 360, 362 (1997); Barbara Bennett Woodhouse, *Hatching the Egg: A Child-Centered Perspective on Parents' Rights*, 14 CARDOZO L. REV. 1747, 1766, 1779–81 (1993).

be taken seriously.[335] Involving children in IoToys decisions could benefit their technological education and improve the parent–child relationship, and the understanding of privacy by both sides.[336] Increasing children's participatory rights, viewed as a positive liberty,[337] could enhance children's liberty and provide considerable privacy protection while affording their independence.[338]

Raising children's awareness of IoToys devices' ability to share their data with their parents should not be generally contested. There is no rationale behind parents knowing children's secrets per se—such knowledge is meant only to safeguard children from revealing personal information that could be misused. Parents could achieve this purpose simply by listening to the communication from the IoToys device—without hearing their child's answer.[339] Also, children must be made aware of the practical—not merely abstract—risks of telling their toy everything. To ensure trust, parents should simply talk to their children and explain that they might access their conversations. The "digital talk" could be important in this context.[340] The participants could together decide, for instance, how to adjust the IoToys device's privacy settings, when applicable, in ways that would best reflect both sides' conceptions of privacy.

Unfortunately, this rather intuitive solution will probably not be achieved easily, as it depends, inter alia, on diverse approaches to parenting. Some parents might disregard their children's notion of privacy and choose not to share such information with them. That is why awareness should be raised not simply by parents but also by the state. Policymakers can raise awareness by design. They can oblige OSPs and toy manufacturers to communicate this information through the IoToys device throughout its use, especially in a toy's first communication with a child. They could also oblige OSPs and toy manufacturers to grant children better control over their shared data by enabling them to listen to and delete their own recordings.[341]

Other regulatory ways of raising awareness could be achieved by investing in informative state-sponsored advertisements directed at children or obliging

---

[335] *See* Davis, *supra* note 307; Leta Jones & Meurer, *supra* note 329.

[336] *See, e.g.*, Yasmeen Hashish et al., *Involving Children in Content Control: A Collaborative and Education-Oriented Content Filtering Approach*, PROC. CHI. ACM 1797, 1797, 1800 (2014).

[337] Under a negative liberty approach, privacy should be viewed as a form of exercising personal choice. *See* Cohen, *supra* note 190, at 1907.

[338] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424–25 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656–58 (1999); *see* Cohen, *supra* note 190, at 1907.

[339] *See, e.g.*, Leta Jones & Meurer, *supra* note 329 ("ToyTalk could display Barbie's side of the conversation to parents without revealing their child's responses.").

[340] For more on educating children on privacy through having the digital "talk" see Priya Kumar, *How to Teach Your Kids About Digital Privacy and Security*, SLATE (Dec. 18, 2017), http://www.slate.com/articles/technology/future_tense/2017/12/giving_your_kids_screen_time_remember_to_talk_to_them_about_digital_privacy.html [https://perma.cc/BW2V-HY9B].

[341] *See* McReynolds et al., *supra* note 234, at 8.

toy manufacturers or IoToys OSPs to include this information in their advertisements. Thereafter the state could also invest in more general awareness-raising campaigns or even promote awareness through the education system.[342] Along with awareness, policymakers must consider the notion of children's autonomous choice within the concept of privacy and include them in the consent process. To this end, policymakers could oblige OSPs to obtain verifiable consent from the parents, but also from the children. Only on fulfilment of this *dual-consent requirement* could IoToys devices be activated. This consent model, while potentially objectionable to many parents, could further foster the protection of children's liberty and autotomy. Children do have legal rights;[343] in the context of privacy and IoToys, they should at least have the right to roll back the invisible boundaries of parental surveillance.

VI. CONCLUSION

IoToys might call for a shift in the perception of the collection and retention of children's information online. These forms of regulation will most likely shape children's conceptions of privacy. Essentially, children need not merely a right to privacy or to be let alone but simply the freedom to play with toys, without realizing that it is actually their parents who are toying with their privacy. Children need a liberty simply to be themselves. To properly mitigate the privacy risks that IoToys entails, policymakers must reevaluate the potential risks of IoToys to children's privacy, including their need to keep secrets from their parents, and strike a proper balance between parents' safeguarding their children from these risks while maintaining children's autonomy. COPPA regulation must therefore be revisited and recalibrated to properly meet the challenges of IoToys. This Article suggests such a form of recalibration by revisiting COPPA's requirements and adjusting them to IoToys. It surveys various methods to promote awareness of the risks of IoToys: redefining the choice mechanism; requiring data minimization and transparency; increasing cybersecurity and enforcement; and finally, acknowledging children's privacy interests by involving children in the process.

Clearly, these practices may merely be a temporary solution for protecting children online and could become obsolete due to technological developments. If we consider IoToys in the broader context of IoT, we might argue that any attempt to safeguard children's privacy in a society racing into a ubiquitous surveillance era would be futile. When children are surrounded by IoT devices that constantly gather data from them, sectoral regulation of devices that target children is perhaps no longer practical. Potentially, IoToys necessitates

---

[342] *See* de Haan, *supra* note 283, at 193 ("Parental mediation might be stimulated by awareness-raising campaigns or by meetings at schools.").

[343] For a discussion on the possession of rights by minors in the United States, see Michele Goodwin & Naomi Duke, *Capacity and Autonomy: A Thought Experiment on Minors' Access to Assisted Reproductive Technology*, 34 HARV. J.L. & GENDER 503, 508, 521–33 (2011).

rethinking the legal framework altogether, not simply recalibrating it. But until such potential reform takes place, children's privacy rights should not be forsaken. At the very least, the implications of IoToys and the internet of children has to be on the agenda of governmental or regulatory entities now, not in the future. Children should play with toys. But these toys should not play with their privacy.