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 respond 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 that 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 as it subjects and normalizes 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 COPPA, this regulatory framework might become obsolete in 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? Finally, what are the consequences for children's privacy of ubiquitous parental

* Senior Lecturer, Faculty of Law, University of Haifa; Faculty Member, the 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. I am much grateful to Meryl Alper, Michael Birnhack, Niva Elkin-Koren, Esther Tabitha Earbin, Michal Gal, Sunny Kalev, Omri Rachum-Twaig, 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.

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 focuses on the privacy concerns that IoToys raise. Part I briefly outlines the evolution of IoToys while examining their capacity to collect and retain data. Then, in reference to the legal framework chosen to protect children from online datafication twenty years ago, the next part 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 evaluate whether such compliance is relevant to IoToys' dangers and challenges. Part III revisits COPPA, challenges it, and in calling for its recalibration offers some practical solutions to IoToys' privacy threats. Thereafter Part IV normatively evaluates children's conception of privacy and argues that IoToys' 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.

CONTENTS

INTRODUCTION 3

I. THE INTERNET OF TOYS 4

A. THE EVOLUTION OF CONNECTED SMART TOYS 5
B. SURVEILLANCE AND DATAFICATION OF CHILDREN IN IOTOYS 11

II. REGULATING PRIVACY WITHIN THE INTERNET OF TOYS 13

A. CHILDREN'S RIGHT TO PRIVACY 14
B. APPLICABILITY OF THE LEGAL FRAMEWORK 19

III. REEVALUATING AND RECALIBRATING CHILDREN'S PRIVACY 27

A. REVISITING CHILDREN'S PRIVACY IN IOTOYS 28
B. RECALIBRATING THE LEGAL FRAMEWORK 31
1. Raising Awareness 34
2. Redefining Choice 39
3. Data Minimization and Transparency 40
4. Toy and Information Security 42
5. Effective Enforcement 45

IV. TAKING CHILDREN'S PRIVACY SERIOUSLY 47

A. PARENTING IN THE IOTOYS ERA 48
B. CHILD DEVELOPMENT AND PRIVACY 51
C. CHILDREN'S CHOICE? 56

CONCLUSION 58

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 massage 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, but now this expanding market offers various types of children-targeted toys and other devices that are both smart and connected to the internet. 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.[3]

IoToys sound almost like every child's dream. But while many benefits might accrue from their use, they may also quickly turn into a nightmare. 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. More closely—and within the scope of this Article—they are also subjected to ubiquitous surveillance and datafication by toy conglomerates, their trusted partners, unauthorized third parties like hackers, and even their parents.[4] In

[1] The term Internet of Things was 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. 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.

[2] *See infra* part I.A.

[3] *See infra* parts I.A-I.B.

[4] 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

other words, these seemingly harmless toys could 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 (COPPA) regulation, which applies to websites that target children under age thirteen or knowingly collect personal information from them.[5] COPPA regulation was devised long before the invention of IoT, 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? 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 I briefly introduces the evolution of IoToys and further examines the datafication of children within it. Part II scrutinizes children's right to privacy on the Federal level under COPPA regulation as to whether it is applicable to IoToys. Then Part III reevaluates children's privacy within the IoToys legal framework and proposes to recalibrate it in keeping with COPPA's requirements. Part IV 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. The final part summarizes the discussion and concludes that children's privacy is of profound importance, especially given a potential movement toward a ubiquitous surveillance era.

I. THE INTERNET OF TOYS

---

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." *See* Roger Clarke, *The Digital Persona and its Application to Data Surveillance*, 10 INFO. SOC. 77, 80 (1994).

[5] *See infra* part II.A.

Toys have existed almost as long as humanity itself. According to archaeologists, they date back at least four millennia.[6] While adults might occasionally play with them, traditional toys mostly appeal 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 the human history, and most likely will continue to evolve for years to come.

Aside from their enjoyment and other potential educational and social benefits,[7] IoToys might also have a dark side. Along with their datamining capabilities, they could be exploited by various entities and eventually harm children and violate their legal rights.[8] For a better understanding of these concerns, the first part briefly tells the story of how toys became interactive from their inception in 1890 to the latest technological developments of IoToys. The second part exposes and evaluates the potential dangers that IoToys raise in general and reviews the datamining practices of key market players in the IoToys industry to prepare the way for evaluating IoToys' 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.[9] 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.[10] Humanity though did not care for Edison's invention at that time, as the toy proved a commercial failure. 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.

A market demand for interactive toys can be traced back to the early 1960s. One of the key examples of this then-new market is pull-string dolls

---

[6] *See* Amber Williams, *FYI: What Is the Oldest Toy in the World?*, POPSCI (Feb. 16, 2012), https://www.popsci.com/science/article/2012-01/what-oldest-toy-world.

[7] *See infra* part I.A.

[8] *Id.*

[9] *See* 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. 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.

[10] *See* Dawson, *supra* note 9.

like Mattel's Chatty Cathy.[11] 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.[12] Years later, other toy manufacturers followed suit by introducing communicative toys like Teddy Ruxpin and Furby.[13] Technology inspired life in toys, as they could now talk to children. But the toy's abilities at this stage were still quite limited. Prior to the development of IoT, where ordinary objects became connected to the internet, communication was still almost entirely one-sided. Even the most communicative toys had tightly limited storage capacity and learning capabilities, and 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,[14] 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.[15] 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.[16] These *connected toys* are designed to connect to the internet or

---

[11] *See* SHARON M. SCOTT, TOYS AND AMERICAN CULTURE: AN ENCYCLOPEDIA 60-61 (2009).

[12] *See* Allie Townsend, *See n' Say*, TIME (Feb. 16, 2011), http://content.time.com/time/specials/packages/article/0,28804,2049243_2048656_2049201,00.html.

[13] Teddy Ruxpin is a "talking" bear which mouth and ears move while "reading" stories from an audio tape cassette. Furby is a toy first released in 1998 by Tiger Electronics Inc. which had the ability to "learn English". *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; *Furby* (1998), http://official-furby.wikia.com/wiki/Furby_(1998) (last visited Feb. 10, 2018).

[14] 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.

[15] *See Kids & the Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs and Battling Robots*, FUTURE OF PRIVACY FORUM - FAMILY ONLINE INSTITUTE 2 (FOSI) (Dec. 2016), 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. 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.

[16] *Id.* at 4.

other devices in order to receive and transmit data.[17] 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 could be attractive to anyone, not just children. IoToys marked the birth of two-way communication toys.

Realizing a potential demand for IoToys, before long the market reacted. In 2015 Mattel collaborated with ToyTalk (later rebranded as PullString, Inc.) to introduce a Barbie doll that "actually listens and talks back."[18] 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.[19] 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.[20]

Hello Barbie clearly marked the beginning of a thriving new market.[21] To name a few examples, following Hello Barbie, Mattel introduced the Hello Barbie Dreamhouse (hereinafter The Dreamhouse), a smart connected home for Barbie dolls;[22] Fisher-Price, a subsidiary of Mattel, introduced a Wi-Fi-connected smart toy bear that "talks, listens, and 'remembers' what your child

---

[17] 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.

[18] *See* Katie Lobosco, *Talking Barbie is Too 'Creepy' for Some Parents*, CNN MONEY (Mar. 12, 2015, 4:11 PM), http://money.cnn.com/2015/03/11/news/companies/creepy-hello-barbie.

[19] *See* Iain Thomson, *Hello Barbie: Hang on, this Wi-Fi Doll Records your Child's Voice?*, REGISTER (Feb. 19, 2015), http://www.theregister.co.uk/2015/02/19/hello_barbie.

[20] *See* Lobosco, *supra* note 18; 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.

[21] It seems that it will not take long before market players expand their variety of IoToys 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; *Smart Toy Revenues to Hit $2.8BN This Year, Driven by Black Friday & Christmas Holiday Sales*, JUNIPER RESEARCH (Nov. 9, 2015), https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-$2- 8bn-this-year.

[22] *See Take a Tour of the First Barbie Smart House*, MATTEL, https://barbie.mattel.com/en-us/about/hello-dreamhouse.html (last visited Feb. 10, 2018).

says and even responds when spoken to";[23] CogniToys introduced various cloud-connected toy dinosaurs that listen to children's questions and answer according to their age;[24] 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.[25] This market appears to be growing continuously.[26]

The children's IoT market had recently expanded beyond toys. This expansion was first only proclaimed early in 2017, under its "Nabi" brand, when Mattel announced its plan to manufacture a smart Wi-Fi-connected speaker for children.[27] This device, named Aristotle, was supposed to be equipped with a microphone, LEDs and a camera,[28] and designed to act like computerized personal assistants akin to Amazon Echo or Google Home,[29]

---

[23] *See 7 Smart Toy® Bear*, FISHER-PRICE, http://fisherprice.mattel.com/shop/Product2_10151_10101_18442_-1 (last visited Feb. 10, 2018).

[24] *See About*, COGNITOYS, https://cognitoys.com/pages/about (last visited Feb. 10, 2018).

[25] 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 visited Feb. 10, 2018); *This is Cayla*, MY FRIEND CAYLA, https://www.myfriendcayla.com/meet-cayla-c8hw (last visited Feb. 10, 2018).

[26] For a prediction on the future of IoToys, see, e.g., Ankush Nikam, *Smart/AI Toys Market Value Share, Analysis and Segments 2017-2027*, FIND MARKET RESEARCH (Aug. 7, 2017), http://www.findmarketresearch.org/2017/08/smartai-toys-market-value-share-analysis-and-segments-2017-2027.

[27] *See* Rob Verger, *Mattel touts Aristotle, an Amazon Echo-style Device for Children*, FOXNEWS (Jan. 4, 2017), http://www.foxnews.com/tech/2017/01/04/mattel-touts-aristotle-amazon-echo-style-device-for-children.html.

[28] *Id*.

[29] 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 which 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-googlefeature-removed-from-chrome-browser/#16d299a44e27; *Top Intelligent Personal Assistants or Automated Personal Assistants*, PREDICTIVEANALYTICSTODAY, http://www.predictiveanalyticstoday.com/top-intelligent-personal-assistants-automated-personal-assistants/#content-anchor (last visited Feb. 10, 2018). More specifically, *Amazon Echo* is "a hands-free speaker you control with your voice." 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

programmed for children's purposes.[30] As for now, Mattel decided that Aristotle is not fit for release, and its future is still uncertain.[31] 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.[32] 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 to the wake phrase.[33] Respectively, Amazon had already entered this market in 2018, introducing the Echo Dot "Kids Edition"—a standard Echo Dot with "parental controls, kid-friendly content, and an optimized experience for kids."[34] All in all, as could be drawn from these innovative projections of new devices, IoT will most likely play a substantive role in children-targeted devices in the foreseeable future.

IoToys present 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 short attention span; encourage active play and toy interaction which

---

word "Alexa" and Echo responds instantly." *See Amazon Echo*, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E (last visited Feb. 10, 2018). *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." *See Get to Know Google Home*, https://madeby.google.com/home (last visited Feb. 10, 2018).

[30] *See* Verger, *supra* note 27. 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*, GUARDIAN (Sept. 22, 2016), https://www.theguardian.com/technology/2016/sep/22/digital-children-smart-toys-technology.

[31] *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.

[32] *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.

[33] 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 supra* note 29.

[34] *See* 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.

might be preferable to passive screen time; foster collaborative play with other children; identify learning difficulties or medical problems; and their software could be updated, hence be economically efficient for parents.[35] On the other hand, IoToys have been criticized for their potential educational, social or psychological drawbacks. To name a few, poor quality of play; potentially harming children's development and impeding child-parent interaction;[36] obstructing children's well-being and healthy development which require real relationships and conversations;[37] and a risk to health from electromagnetic radiation (EMR).[38]

IoToys' potential drawbacks do not stop there. They might subject children to various risks, for example, exposure to harmful content.[39] There is even the danger of mental and bodily harm by predators who have gained access to the toy and used it to listen, watch, track, and even directly contact children.[40] Along with these important challenges, these IoToys further raise

---

[35] *See* Stéphane Chaudron et al., *Kaleidoscope on the Internet of Toys: Safety, Security, Privacy and Societal Insights*, JRC TECHNICAL REPORT 9 (2017), http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf; *5 Benefits of Tech Toys for Children*, ROBO WUNDERKIND, http://robowunderkind.com/blog/benefits-tech-toys-kids (last visited Feb. 10, 2018).

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

[37] *See, e.g.*, Richard Chirgwin, *Mattel's Parenting takeover continues with Alexa-like Dystopia*, REGISTER (Jan. 4, 2017), https://www.theregister.co.uk/2017/01/04/mattels_parenting_takeover_continues_with_alexalike_dystopia.

[38] *See* Chaudron et al., *supra* note 35, at 9.

[39] 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. *See Amazon Alexa Gone Wild*, YOUTUBE (Dec. 29, 2016), https://www.youtube.com/watch?v=r5p0gqCIEa8 (last visited Feb. 10, 2018). 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*, HUFFINGTON POST (Feb. 9, 2015), http://www.huffingtonpost.com/2015/02/09/my-friend-cayla-hacked_n_6647046.html?utm_hp_ref=weird-news&ir=Weird+News.

[40] 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)*,

human rights concerns. Potentially they can subject children to ubiquitous surveillance and datafication, which could profoundly impact their right to privacy.[41] To normatively assess the privacy challenges—which is core purpose of this Article—the next part briefly reviews 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 may evince wide differences.[42] Some are smarter than others. Some are equipped with more technological tools that enhance their capabilities; others are simply more sophisticated, for example, are equipped with a microphone, while others have cameras and other sensors. Some, like Hello Barbie, require their users to turn them on manually, while others, like the Dreamhouse and the Hologram, operate in an "always on" mode, namely constantly operate as they await their wake phrase. Yet their different characteristics notwithstanding, the core functions of IoToys are fairly similar: upon activation, the 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.[43] Barbie Products capture recordings upon users' interaction with them, whether by pressing the "talk" button or saying the wake phrase.[44] Other products, like Cayla, also capture their users' recording, usually after a wake phrase. 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

---

DAILY BEAST (Dec. 10, 2015), http://www.thedailybeast.com/hackable-hello-barbie-the-worst-toy-of-the-year-and-maybe-ever. For a typology of risks to children online, *see* THE PROTECTION OF CHILDREN ONLINE - RECOMMENDATION OF THE OECD COUNCIL REPORT ON RISKS FACED BY CHILDREN ONLINE AND POLICIES TO PROTECT THEM (2012), https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf.

[41] For more on children's right to privacy, see *infra* part II.A.

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

[43] *See Privacy Policy*, TOYTALK, https://www.toytalk.com/hellobarbie/privacy (last visited Feb. 10, 2018) (hereinafter: ToyTalk Privacy).

[44] *See* ToyTalk Privacy, *supra* note 43 ("When a child interacts with the product (by clicking the button or saying the gate phrase) the voice recordings may be captured.").

identifier; Wi-Fi password; and mobile device information.[45] Essentially, most of these IoToys 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.[46] Obviously, data can be highly valuable for various interested parties for a variety of business purposes, much like any data that is gathered online.[47] It can potentially be commercialized and shared with other interested parties.[48] From a functional aspect, data could be valuable for the toy's improvement. As some toy manufacturers and OSPs posit, the entertainment experience from the toy is to some extent based on the audio recordings sent from it, which are then analyzed and stored.[49] 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;[50] likewise the development of acoustic and

---

[45] *See Children's Connected Toys: Data Security and Privacy Concerns*, COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION 12 (Dec. 14, 2016), https://www.billnelson.senate.gov/sites/default/files/12.14.16_Ranking_Member_Nelson_Report_on_Connected_Toys.pdf. Images and audio, however, are currently only stored locally on the bear. *Id.*

[46] 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 voice recordings." *See, e.g.*, ToyTalk Privacy, *supra* note 43. As for the Hologram, however, Mattel announced that it does not save the recordings in its servers. *See* Moynihan, *supra* note 32.

[47] *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 (2005).

[48] 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 25. 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 43; FAQ, TOYTALK, https://toytalk.com/legal (last visited Feb. 10, 2018).

[49] ToyTalk claim 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*, GUARDIAN (May 26, 2016), https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law. It should also be further noted that ToyTalk archive users' play sessions. *See* FAQ, *supra* note 48.

[50] *See* ToyTalk Privacy, *supra* note 43; *Privacy Policy*, *supra* note 25.

language models.[51] It might also be necessary for other research, development and data analysis purposes.[52] 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 toy. Toys equipped with sensors could give third parties access to data in real-time from these sensors. Toys with a GPS tracker let third parties know where the toy is currently located and where it has been since it was first configured. And finally, toys equipped with a camera could enable third parties to see what the toy is 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 their existence and development, it also raises substantial privacy concerns . How can we properly safeguard the data that is aggregated through IoToys from authorized and unauthorized entities that have gained access to the data? Does the current American legal framework[53]—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.

II. REGULATING PRIVACY WITHIN THE INTERNET OF TOYS

It is generally uncontested that children require special care and assistance.[54] As a cohort, they are less equipped with the skills and cognitive ability to

---

[51] *See* ToyTalk Privacy, *supra* note 43.

[52] *Id*.

[53] 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, e.g., Daniel J. Solove & Paul M. Schwartz, *An Overview of Privacy Law in* PRIVACY LAW FUNDAMENTALS 145-56 (IAPP, 2015).

[54] Many consider childhood to be entitled to special care and assistance. On the global level, see 'Convention on the Rights of the Child', United Nations, Adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989. In the EU, the General Data Protection Regulation (GDPR) sets higher standards (than adults) for all collection, use and disclosure of data when children's data are sometimes involved. Article 8 of the GDPR sets a parental consent requirement for all children aged under sixteen where online services are offered directly to them; EU member states can lower the age threshold to thirteen. Consequently, Recital 38 requires prior parental consent before

comprehend some risks and concerns as adults do, let alone the depth and complexity of human rights and liberties.[55] They might lack the requisite maturity, ability, knowledge and experience to properly protect themselves, and could be more trusting than adults.[56] They might value their immediate needs more than their long-term interests;[57] not understand the true nature or appropriate use of the collected information;[58] and value privacy differently from their parents.[59] In other words, while accounting for potential age differences, children often need guidance on various aspects of their lives, including how properly to protect their privacy.

A. Children's Right to Privacy

There are many different views on what privacy means and how best to protect it.[60] The modern concept of privacy is generally attributed to the famous Law Review Article by Samuel Warren & Louis Brandeis, published in the same year that Edison introduced the first-ever talking doll, which articulated the

---

processing of children's personal data. *See* Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive 95/46/EC, Art. 83, 2016 O.J. L 119/1. For more on EU's perception of children's privacy see generally 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. 765 (2017); Sonia Livingstone, *Children: a special case for privacy?*, 46 INTERMEDIA 18 (2018). For a detailed report on online risks to children, see John Palfrey et al., *Enhancing Child Safety and Online Technologies: Research Advisory Board Report for the Internet Safety Technical Task Force*, BERKMAN CTR. FOR INTERNET & SOC'Y (2008), http://cyber.law.harvard.edu/pubrelease/isttf.

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

[56] *See* Danielle J. Garber, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 132 (2002); Dorothy A. Hertzel, *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).

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

[58] *See* Jerry S. Birenz, *Caching World Wide Web Sites*, 516 PRACT. L. INST. 475, 516 (1998); Hertzel, *supra* note 56, at 434.

[59] *See* Emily Nussbaum, *My So-Called Blog*, N.Y. TIMES, Jan. 11, 2004 § 6 (Magazine), at 32, 34. For more on children's perception of privacy *see infra* part IV.B.

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

right to privacy as the "right to be let alone."[61] 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;[62] "limited access theory" which posits that privacy is related to our concern about our accessibility to others;[63] and a conceptual framework of privacy as contextual integrity which links the protection of personal information to the norms of specific contexts.[64] 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 perception of what is known as sectoral privacy.[65]

American policymakers chose this sectoral approach to privacy, seeking to provide legal safeguards that would presumably improve children's safety online and reasonably secure their privacy.[66] In 1998, under this

---

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

[62] *See generally* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) ("[T]he claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others.").

[63] *See generally* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980); ANITA ALLEN, UNEASY ACCESS: PRIVACY FOR WOMAN IN A FREE SOCIETY (1988).

[64] *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).

[65] 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 for instance, Fair Credit Reporting Act, Pub. L. No. 91–518, 84 Stat. 1129 (1970) (codified as amended at 15 U.S.C. §§ 1681, 1681a–1681x (2012)) and Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. §§ 6801-09 (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). *See generally* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003).

[66] 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." *See* INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION 5 (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,

perceived need to protect children's privacy online,[67] Congress enacted the Children's Online Privacy Protection Act (COPPA).[68] To supplement COPPA, the Federal Trade Commission (FTC) issued a rule, last updated in 2013, which is commonly referred to as the "COPPA Rule."[69] 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.[70]

Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 STAN. L. REV. 1315 (2000).

[67] 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, 168-69 (3d Cir. 2000).

[68] 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 (last visited Feb. 10, 2018); *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 (2015).

[69] *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 is effective since April 2000. For the latest update see 78 Fed. Reg. 3972 (Jan. 17, 2013).

[70] 15 U.S.C. §§ 6501-6505 (2012); Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2012)); Garber, *supra* note 56, 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." Substantial injury, in this instance, could apply on both financial harms and unwarranted health and safety risks. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014); Fed. Trade Comm'n v. Information Search, Inc., Civ. No. 1:06-cv-01099 (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).

COPPA regulation applies to Online Service Providers (hereinafter OSPs) that target children under age thirteen[71] or knowingly collect personal information from them.[72] 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.[73] 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.[74]

As a form of market self-regulation—commonly termed *privacy self-management*,[75] COPPA incorporates five essential Fair Information Practice Principles (FIPPs):[76] notice, choice, access, security, enforcement.[77] Websites that fall under COPPA regulation must include a *notice* containing what information is collected, how it is used, and its information disclosure

---

[71] 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, e.g, Bartolia, *supra* note 57, at 38.

[72] Personal information is defined as individually identifiable information about an individual collected online, including: (1) Full name; (2) 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) Screen or user name where it functions in the same manner as online contact information, as defined in this section; (5) Telephone number; (6) 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) Other information about the child or parent that is collected from the child and is combined with one of these identifiers. *See* 16 C.F.R. § 312.2 (2012); 15 U.S.C. §§ 6501(1), 6502, 6501(8) (2012).

[73] 15 U.S.C. § 6501 (2012).

[74] *Id*.

[75] Privacy self-management is an approach to privacy regulation whereas the law provides people with a set of rights, e.g., primarily of 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, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013).

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

[77] FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May, 2000) at i, 3, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf; Garber, *supra* note 56, at 153.

practices.[78] OSPs must obtain *verifiable parental consent* for the collection, use, or disclosure of such personal information.[79] 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 *to refuse further use or maintenance or future online collection* of personal information from that child.[80] The operator must also provide reasonable means, in the given circumstances, for the parent *to obtain any personal information collected from that child*.[81] 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.[82] 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.[83]

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.[84] Consequently it can issue fines and seek preliminary or permanent injunctive remedies for those who do not comply with COPPA regulation.[85] While to date most cases have resulted in settlement

[78] 15 U.S.C. § 6502(b)(1)(A)(i) (2012).

[79] *Id*. § 6502(b)(1)(A)(ii).

[80] *Id*. § 6502(b)(1)(B).

[81] *Id*. § 6502(b)(1)(B).

[82] *Id*. §§ 6502(b)(1)(C)-(D).

[83] 16 C.F.R. § 312.3(e) (2012).

[84] 15 U.S.C. §§ 6501–6506 (2012). The FTC authority stems from both The Federal Trade Commission Act (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 Procedures Act (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 70, at 588.

[85] 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. *See* Shaun Nichols, *Viacom, Mattel and Pals Busted for Stalking Kids with Creepy Web Ads*, REGISTER (Sept. 14, 2016), http://www.theregister.co.uk/2016/09/14/viacom_mattel_busted_for_tracking_kids. Violating COPPA requirements could currently lead to fines up to $40,000 per violation. *See* Federal Trade Commission, *Adjustment of Civil Monetary Penalty Amounts*, 81 Fed. Reg. 42476 (June 30, 2016).

agreements,[86] the FTC reported that up to 2016 it brought over twenty COPPA cases and collected millions of dollars in civil penalties.[87]

COPPA has received much scholarly attention since its inception,[88] but it now extends far beyond regulation for the internet. Being online in 2018 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.[89] This second category encompasses gathering any personal information from a child, including requesting, prompting, or encouraging a child to submit personal information; enabling a child to make personal information publicly available in identifiable form; passive tracking of a child online; and real-time physical locations of

---

[86] *See* Solove & Hartzog, *supra* note 70, at 585. The FTC reported that concerning data security, they entered into approximately sixty settlements related to companies' failure to protect consumers' personal information. *See* Letter to Senator Warner (June 22, 2017), https://www.scribd.com/document/352278126/2017-06-21-Response-to-Senator-Warner-Letter.

[87] *See* Federal Trade Commission, *Privacy and Data Security Update (2016)*, https://www.ftc.gov/reports/privacy-data-security-update-2016#children (last visited Feb. 10 2018).

[88] While many articles that relate to COPPA are further cited within this Article, here are few examples of such scholarly work: Joshua Warmund, *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); 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 (2001); Garber, *supra* note 56; Solove & Hartzog, *supra* note 70.

[89] *See* 16 C.F.R. § 312.2 (2012).

children.[90] Children's data in IoToys easily fall within these definitions. The mere use of IoToys that children can talk to should be deemed a way of encouraging the child to submit personal information.[91] 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.[92]

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.[93] 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, will not generally generate sensitive information.[94] It might be presumptuous to assume that all IoToys 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.[95] In addition, when a device enables recording and transmitting data, it could potentially capture personal

[90] 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. *See id*.

[91] *Id*. §§ 6502(b)(1)(C)-(D).

[92] *See Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FTC (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (last visited Feb. 10, 2018). *See also* Letter to Senator Warner, *supra* note 86 ("The COPPA Rule applies not only to websites, but also to other online services, including connected toys and associated mobile apps.").

[93] 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.

[94] It should, however, be further noted that under the mosaic theory, even data which seemingly non-sensitive might become one due to aggregation. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (introducing the mosaic theory). For more on the mosaic theory, see Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 314 (2012); David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 390 (2013); Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 4 (2012); Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 146-52 (2017).

[95] *See* 16 C.F.R. § 312.2 (2012).

data such as the name, home address, online contact information and even social security numbers of children, and thus might also trigger COPPA.

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 five requirements: (1) notice; (2) verifiable parental consent; (3) the right of parental review of such information; (4) prohibition against conditioning a child's online activity—against the child disclosing more personal information than is reasonably necessary to participate in such activity; and (5) establishing and maintaining adequate and reasonable security policies.[96] To enjoy safe haven from enforcement action under COPPA regulation, companies could also follow self-regulatory guidelines pre-approved by the FTC.[97] As for the latter, without transparency of FTC-approved practices,[98] 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.[99]

The first component is *notice*.[100] This form of regulation-by-information is a well-known practice in many markets.[101] Under it, consumers

---

[96] 15 U.S.C. § 6502 (2012); 16 C.F.R. §§ 312.3(a)-(e) (2012); 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).

[97] To gain a safe harbor approval, companies must meet or exceed the five statutory requirements identified above; include an "effective, mandatory mechanism for the independent assessment of . . . compliance with the guidelines"; and 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. *See* 15 U.S.C. § 6503 (2012); 16 C.F.R. § 312.11 (2012); Rubinstein, *supra* note 96, at 395.

[98] While the FTC announced that it approved applications like the iKeepSafe Safe Harbor Program, it is difficult to assess their practices without transparency. *See Commission Letter Approving Application of iKeepSafe Safe Harbor Program for Approval of its Children's Online Privacy Protection Rule Safe Harbor Program*, FTC (Aug. 1, 2014), https://www.ftc.gov/system/files/documents/public_statements/573811/140806ikeepsafeapp.pdf.

[99] It should be noted that Hello Barbie is currently certified by the FTC as COPPA compliant under the kidSAFE Seal Program. *See infra* note 186. 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.

[100] 16 C.F.R. § 312.3(a) (2012).

[101] 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. Under such regulatory mechanism, the "discloser" gives the "disclosee" information, and the later can make better decisions for him, and likewise reduce the "power" of the former to control the later. For examples of disclosure requirements set by legislation,

must be apprised of the various implications of using a product they have purchased or a service they registered to. As COPPA applies to the internet, regulators require that a notice must be posted on the Website.[102] A link to the notice must be prominent and clearly labeled, and appear on the home or landing page or screen of its services where personal information is collected from children.[103] The notice must include what information is collected from children, how the operator uses such information, and the operator's disclosure practices for such information.[104] It must also be clear and understandable and in writing,[105] and the OSP must make reasonable efforts directly to notify parents regarding its practices.[106]

Many of the key-market players, like ToyTalk for instance, are found largely to comply with the notice component. 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.[107] While its evaluation is subjective, it also uses clear and understandable language.[108]

---

see Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA L. REV. 647, 649-50 (2011). 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).

[102] 15 U.S.C. § 6502(b)(1)(A)(i) (2012).

[103] The link must be in close proximity to the requests for information in each such area. *See* 16 C.F.R. § 312.4(d) (2012).

[104] 15 U.S.C. § 6502(b)(1)(A)(i) (2012).

[105] 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."). The online notice of the website or online service's information practices must state the (1) 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. *See id*. § 312.4(d).

[106] Including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented. *See id*. §§ 312.4(b)-(c).

[107] *See ToyTalk*, https://www.toytalk.com (last visited Feb. 10, 2018); *Hello Dreamhouse™ Companion App*, https://www.toytalk.com/product/hello-house (last visited Feb. 10, 2018); *Hello Barbie™ Companion App*, https://www.toytalk.com/product/hello-barbie (last visited Feb. 10, 2018).

[108] *Id*.

Genesis, however, might fulfill this requirement less. Cayla's homepage currently does not contain such a link. Nor does the App store, when the designated App is downloaded.[109] Cayla's privacy policy is only visible after a user goes to the "More" section on the top menu.

The second component of COPPA requires *verifiable parental consent*,[110] namely more than implied parents' consent, for the collection, use or disclosure of personal information obtained from children.[111] The parent must receive notice of such use and authorize the collection, use or disclosure of the personal information,[112] and must have the option not to consent to disclosure of information to third parties.[113] The steps for verifiable parental consent are vaguely articulated as "*any reasonable effort* (taking into consideration available technology), including a request for authorization."[114] 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*.[115] In addition, the FTC could approve other methods that satisfy the parental consent requirement.[116]

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.[117] Currently, parental consent for

---

[109] *See My friend Cayla App (EN-US)*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.toyquest.Cayla.en_us (last visited Feb. 10, 2018); ITUNES STORE, https://itunes.apple.com/app/id984342622 (last visited Feb. 10, 2018).

[110] 16 C.F.R. § 312.3(b) (2012).

[111] 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)(1)(D)(2)(A)-(C) and 16 C.F.R. § 312.5 (2012).

[112] 16 C.F.R. § 312.2 (2012).

[113] *Id*. § 312.5(a)(2).

[114] 15 U.S.C. § 6501(9) (2012).

[115] Under this method, the OSP sends an email to the parent and have them respond with their consent. The OSP then sends a confirmation to the parent (via email, letter, or phone call). OSPs must also notify the parents how to revoke their consent at any given time. *See Children's Online Privacy Protection Rule, supra* note 92.

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

[117] These methods also 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; verifying a parent's identity by

Barbie products is obtained by one's creating an account and accessing the services of ToyTalk.[118] 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.[119] It further states: "If you do not agree to this, please do not use our website or provide us with any information."[120] Genesis however notes that it will not knowingly accept any information by any children under age thirteen without the express permission of their parent or guardian.[121]

The third step is *right of parental review.*[122] At a parent's request, OSPs are required to provide three things: a description of the specific types or categories of personal information collected from children by the operator;[123] they must grant parents the opportunity to refuse further use or future collection of personal information, and must grant the option of deleting the gathered information;[124] and they must grant parents the right to review the collected information.[125]

For Barbie products, ToyTalk specifies that parents have the right to review or delete any personal information collected from their child that it retains. Parents also have the right to review and delete any audio files in their

---

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; or, if the OSP does not disclose children's personal information (as defined by § 312.2) they may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent (e.g., 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). *See id.* § 312.5.

[118] *See* ToyTalk Privacy, *supra* note 43 ("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.").

[119] *See Privacy Policy*, GENESIS-TOYS.COM, https://www.genesis-toys.com/privacypolicy (last visited Feb. 10, 2018).

[120] *Id*.

[121] *See Privacy Policy*, *supra* note 25.

[122] 16 C.F.R. § 312.3(c) (2012).

[123] Exampled are name, address, telephone number, email address, hobbies, and extracurricular activities. *See id*. § 312.6(a)(1).

[124] *Id*. § 312.6(a)(2).

[125] To comply, considering available technology, OSPs must ensure that the requestor is a parent of that child, and not be unduly burdensome to the parent. *See id*. § 312.6(a)(3).

account and may also permanently delete their accounts via the website.[126] Even lacking a request, ToyTalk claims that it will delete personal information that children provide when it becomes aware of it, and contractually oblige its service providers to act similarly.[127] 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 the right to access information it holds about them.[128] 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 offer of a prize, or any other activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.[129] This step might be trickier in respect of IoToys than of 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. 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. 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*.[130] OSPs are obliged to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.[131] Releasing the information to a third party requires ensuring that they take similar steps to protect the data, and that they can vouch for these measures.[132] To reduce the risk of privacy violations in a cyber

---

[126] *See Hello Barbie and Hello Dreamhouse Privacy FAQ*, TOYTALK, https://www.toytalk.com/hellobarbie/privacyfaq (last visited Feb. 10, 2018).

[127] *See* FAQ, *supra* note 48.

[128] *See Privacy Policy*, *supra* note 25.

[129] 16 C.F.R. § 312.3(d) (2012).

[130] *Id*. § 312.3(e).

[131] *Id*.

[132] *Id*. § 312.8. *See also Children's Connected Toys*, *supra* note 45, at 5-6.

security breach, the FTC also imposes on OSPs data retention and deletion requirements.[133]

Surveys have shown that many IoToys' OSPs implement data security measures in their toys.[134] Barbie products use secure, encrypted communications when transferring all personal information over the web. Wi-Fi credentials are stored in an encrypted section so that the products can connect to the internet.[135] The Hello Barbie Hologram uses 256-bit encryption when it sends queries to the cloud.[136] 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."[137]

Are these security policies reasonable? Difficult to say, as it depends on the toy in question.[138] But in practice they are found not secure enough: IoToys has often been breached since its inception,[139] including Hello Barbie.[140]

---

[133] 16 C.F.R. § 312.10 (2012).

[134] Including, but 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. *See Children's Connected Toys*, *supra* note 45, at 9.

[135] *See* ToyTalk Privacy, *supra* note 43.

[136] *See* Moynihan, *supra* note 32. It should be noted that Aristotle was supposed to use encryption to keep at least some form of information private. 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. They also declare that baby cameras utilize IP addresses or radio frequency to deliver data and communication streams that are easily hacked or intercepted. *See Aristotle*, 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.

[137] *See Privacy Policy*, *supra* note 25.

[138] For an analysis of security flaws in IoToys, *see generally* Valente & Cardenas, *supra* note 42, at 19.

[139] *See, e.g.*, Lorenzo Franceschi-Bicchierai, *One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*, MOTHERBOARD (Nov. 27, 2015), http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids (breach of consumer data to VTech Electronics North America, a maker of children's connected tablets); Mark Stanislav, *R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy® & hereO GPS Platform Vulnerabilities (FIXED)*, RAPID7 (Jan. 25, 2016), https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform; Danny Yadron, *Fisher-Price Smart Bear allowed Hacking of Children's Biographical Data*, GUARDIAN (Feb. 2, 2016), https://www.theguardian.com/technology/2016/feb/02/fisher-price-mattel-smart-toy-bear-data-hack-technology (noting that the app connected to the Fisher-Price toy had several security

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 breach. A recent example concerns VTech Electronics Limited, an electronic toy manufacturer, which experienced a major cybersecurity breach. Only then did consumers learn that their children's data was not encrypted even though the firm's privacy policy stated that it was.[141]

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 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' challenges is suggested.

III. 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

---

flaws that would allow hackers to obtain data); Alex Hern, *CloudPets Stuffed Toys leak details of Half a Million Users*, GUARDIAN (Feb. 28, 2017), https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults (describing a data breach that compromised personal information of more than half a million people who bought the toys).

[140] Hackers showed how they hijacked a Hello Barbie. *See* Samuel Gibbs, *Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children*, GUARDIAN (Nov. 26, 2015), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children; Richard Chirgwin, *Hello Barbie Controversy re-ignited with Insecurity Claims*, REGISTER (Nov. 29, 2015), http://www.theregister.co.uk/2015/11/29/hello_barbie_controversy_reignited_with_insecurity_claims. 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. *See* 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.

[141] VTech eventually settled with the FTC and was obliged to pay $650,000 for COPPA violation. *See Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act*, FTC (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

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 IoToy realm.

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 era when policymakers sought to protect the privacy of personal information collected from and about children on the world wide web. The need to protect children's privacy not only exists in IoToys, but is actually greater. It is based on the core differences between the internet and IoT in general, where IoT increases 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.[142] More closely, IoToys 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. It does so simply by adding another form of connection to the internet. Arguably however, children might view IoToys 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 difficult to see these two different

[142] *See* Shackelford *supra* note 1, at 427.

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 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 verbal, 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.[143] This relates to younger children, but also to those who experience difficulty writing or reading, so these toys offer them access to the internet.

Another factor that increases volume is computer or technological illiteracy.[144] As a core argument, children, at least young ones, might be more accustomed to play with toys than use a computer, hence IoToys will appeal to them more and be generally easier to use. Notably, however, this argument might become less relevant for digital natives[145] as the use of computers like smartphones or tablets might begin at relatively early stages of their lives.[146] Still, after the setup step, usually undertaken by the child's parent, operating IoToys like Hello Barbie or Cayla is generally easier and quicker than using the internet via computers. Perhaps IoToys 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, so connection to the

---

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

[144] 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).

[145] While these definitions evolve over time, the term digital natives generally refer to those who grew-up in the digital age, in oppose to the digital immigrants. For more on these terms, see Marc Prensky, *Digital Natives, Digital Immigrants*, 9 ON THE HORIZON 1 (2001); JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008).

[146] As reported by Common Sense Media, a nonprofit organization, in 2017, 42% of American children aged eight or younger, have their own tablet devices. *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. *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-secondarystudents-use-school-issued-mobile-devices.aspx.

internet can be via laptops, mobile phones, tablets, and other connected devices. Nevertheless, parents might decide to limit their children's accessing the internet, especially young ones, to a computer that is fairly visible to them. IoToys' 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. 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 Technologies (PET)—designed to enhance users' privacy.[147] 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.[148] 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. They might, for instance, conceive their toy to be their new best friend and form an attachment.[149] Children might even anthropomorphize

---

[147] A good example of PETs are Communication anonymizers and Enhanced Privacy ID (EPID), a digital signature algorithm supporting anonymity. Other examples include the Platform for Privacy Preferences ("P3P") designed to provide "smarter Privacy Tools for the Web." Essentially, P3P is a protocol that allows websites to declare their intended use of information they collect. *See Platform for Privacy Preferences (P3P) Project*, W3C, https://www.w3.org/P3P (last visited Feb. 10, 2018). A final example is the *TrackMeNot* browser plug-in, which sends 'decoy' queries to popular search engines whenever a user searches them while generating algorithmic 'noise'. *See* 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.

[148] Examples in the early 2000s included computer programs like Cybersitter and NetNanny. *See* Hertzel, *supra* note 56, at 447-48.

[149] Upon initiation, Hello Barbie explicitly communicates that to the user. Upon asking the child's name, Hello Barbie would reply "I just know we're going to be great friends." *See* Vlahos, *supra* note 9.

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).[150] 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 be also further challenged that anthropomorphizing these toys might actually lead to children not trusting them, or rather, tell them lies. Still, along with developments in IoToys, their ability to offer more types of interactive games should 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 should not differ greatly, depending on their marketing purposes. Unauthorized access, however, is generally facilitated in IoToys due to potential security flaws. 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' 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. 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—or simply even adds another form of data mining on children (apart from the internet); that this information might be more sensitive; and might be 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 OSPs 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

[150] Doris Bergen argued that it is very difficult for children, especially young ones, to distinguish what is real from what is not. *See 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).

the IoToys market, regulating IoToys requires acknowledging the differences between them and the internet. Examining the current COPPA requirements in light of these differences clearly shows how inadequate it currently is to safeguard children properly from privacy risks. This inadequacy must be further addressed by recalibration.

As a general argument, one might argue that the legal framework of sectoral privacy in general is no longer applicable in this age. That the U.S. should take the path chosen by the EU and embrace an omnibus privacy regime.[151] That it is not wise to keep updating laws such as COPPA due to the rise of new technologies, but rather craft technology neutral laws.[152] While such moves could very well be advisable, this Article will not undertake this important theoretical debate—but 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 U.S. 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,[153] but by the present interpretation of the Supreme Court, it will not extend to non-state actors, which include IoToys manufacturers and OSPs, so information privacy will not generally be protected by it.[154] Accordingly, tort law will be fairly limited to deal with the risks of IoToys as it mainly deals with disclosure of embarrassing personal information and not simply the collection and use of personally identifiable information.[155] Consumer protection law could be invoked to some extent, but

---

[151] *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1764 (2010). *Cf.* Paul M. Schwartz, *Preemption and Privacy*, 18 YALE L.J. 902 (2009) (discussing the drawbacks of embracing an omnibus privacy regime in the U.S.).

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

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

[154] 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 for this protection includes prohibiting unreasonable searches and seizures and freedom of assembly. Invoking constitutional rights, however, requires that a state action be present. Thus, these rights protect citizens against the government, while they fail to grant protection for citizens against each other (including against private companies). *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 501-03 (1995).

it will mainly deal with the IoToy itself, and less with the practices of safeguarding the stored data at least on the Federal level.[156]

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 supply sufficient measures to protect children's privacy. An obvious ex-ante solution for reducing the potential risks of IoToys, 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.[157] In the IoToys market, German authorities embraced this approach recently when they decided to ban the IoToy Cayla due to its (proclaimed) inherent security flaws.[158] Germany's Federal Network Agency even took this approach a step farther 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.[159]

---

[155] The right to privacy could be protected to some extent by tort law under four branches: (1) misappropriation of name or likeness for commercial purposes, (2) the public disclosure of private facts; (3) intrusion upon seclusion; and (4) false light publicity. *See* Restatement (Second) of Torts § 652 (1977); William Prosser, *The Right to Privacy*, 48 CALIF. L REV. 383, 389 (1960). Establishing a tort claim under this 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; public disclosure of private facts protects against the circulation to the general public of offensive information (that is not otherwise publicly available); and false light protects against wide dissemination of information that is misleading or erroneous. What might be relevant is intrusion upon seclusion which protects against highly offensive methods of gathering information in private areas. For more on torts and privacy, see Reidenberg, *supra* note 154, at 504-06; Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1291 (2000).

[156] 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*, 2011 EUR. J. CONSUMER L. 853 (2011).

[157] *See World: Americas Furby Toy or Furby Spy?*, BBC NEWS (Jan. 13, 1999), http://news.bbc.co.uk/1/hi/world/americas/254094.stm.

[158] *See* 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.

[159] *Id.* Notably, Germany also recently banned children's smartwatches. *See* Jane Wakefield, *Germany bans Children's Smartwatches*, BBC NEWS (Nov. 17, 2017), http://www.bbc.com/news/technology-42030109.

This Article does not support such solutions as an agenda and they are also highly unlikely in the U.S.. Beyond the potential benefits to children, IoToys could be valuable for technological developments and innovation.[160] 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,[161] and it could further lead to social benefits and the enhancement of social welfare.[162] Thus, heavily regulating the flow of information, let alone banning IoToys altogether, could stifle innovation and should be carefully examined.[163]

Instead of banning IoToys, policymakers should consider other, less-restrictive, legal measures, which could lessen the risks that IoToys entail while preserving their benefits. To achieve such a balance, policymakers must combine ex-ante and ex-post measures, by allowing developments in IoToys, while setting a framework in which these toys operate, are manufactured and sold, and especially in which it is seen how data is used, by whom and for which purposes. Essentially, COPPA regulation attempts to do this precisely, but as previously mentioned, it requires far-reaching modifications to its requirements.

1. *Raising Awareness*

Any legal guardian, even without purchasing IoToys, must be aware of their potential implications. They must certainly understand the risks of IoToys to information privacy and security by understating the information the OSP collects, how it will be used, whether it will be shared, and if so with whom, and how long the information will be retained.[164] 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 play with an IoToy without their knowledge or consent.[165]

---

[160] For a comprehensive analysis of the privacy-innovation debate, see Tal Zarsky, *The Privacy-Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 116 (2015). In the context of big data, see Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1918–27 (2013).

[161] *See* Zarsky, *supra* note 160, at 118.

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

[163] *See* Zarsky, *supra* note 160, at 118.

[164] *See Children's Connected Toys*, *supra* note 45, at 2.

[165] The notions of awareness and consent in IoToys might be also perceived tricky due to secondary users. What happens, for instance, when a child uses his friend's IoToy, consented

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' privacy risks, thereby reducing the discloser's power to control the disclosee by granting them informed choice on whether to use this product.[166] While COPPA promotes this type of regulation by its notice requirement,[167] 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.[168] When the internet is embedded in the operation of devices, direct exposure to a website does not exit, 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 raise awareness properly.

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

---

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 IoToy 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). *See Archer-Hayes v. Toytalk, Inc.*, No. 2:16-cv-02111-JAK-PLA (C.D. Cal. Dec. 7, 2015). From a legal certainty perspective, this case was unfortunately voluntarily dismissed, leaving void on the applicability of secondary use within IoToys. *See* Stipulation of Voluntary Dismissal with Prejudice, *Archer-Hayes v. Toytalk, Inc.*, No. 2:16-CV-2111 (C.D. Cal. July 22, 2016), ECF No. 42. It is generally still unclear whether a secondary use of an IoToy 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 IoToy). 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. *See* ToyTalk Privacy, *supra* note 43 ("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.").

[166] *See generally*, Ben-Shahar & Schneider, *supra* note 101; BEN-SHAHAR & SCHNEIDER, *supra* note 101.

[167] 16 C.F.R. § 312.3(a) (2012).

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

carefully to read disclosures and privacy policies.[169] 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),[170] most consumers do not bother to read them;[171] they are usually long[172] and written in a legal language almost incomprehensible to most people; likewise privacy policies or notices.[173] Most people do not see, read or understand them, and they might also be changed frequently.[174] Even shortening these policies might only insert marginal improvements to make them more comprehensible,[175] and they might also leave out important information to make any consent truly informed.[176]

---

[169] *See Public Service Announcement*, FBI (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx.

[170] The use of ToS and EULAs are merely to exemplify how individuals treat vast amount 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 mainly the province of the FTC. *See* Solove & Hartzog, *supra* note 70, at 589. For attempts to enforce privacy policies as contracts, see, e.g., 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, 1999–2000 (D.N.D. 2004).

[171] Ben-Shahar & Schneider, *supra* note 101, at 665–78; Solove, *supra* note 75, at 1885; Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 930 (2013).

[172] *See, e.g.*, Daniel B. Ravicher, *Facilitating Collaborative Software Development: The Enforceability of MassMarket Public Software Licenses*, 5 VA. J.L. & TECH. 11, 13 (2000); Garry L. Founds, *Shrinkwrap and Clickwrap Agreements: 2B or Not 2B?*, 52 FED. COMM. L.J. 99, 100 (1999).

[173] For studies on privacy notices, see, e.g., NISSENBAUM, *supra* note 64, at 105; 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); 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 540 (2008); *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is.

[174] *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160 (1999) ("[N]o one has the time or patience to read through cumbersome documents describing obscure rules for controlling data."); 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); Solove, *supra* note 75, at 1885; Ohm, *supra* note 171, at 930.

[175] *See, e.g.*, Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1033 (2012).

[176] *See* Solove, *supra* note 75, at 1885.

Essentially, individuals already experience information flooding and are unlikely to spend time or effort on reading these polices.[177]

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.[178] It is beset with cognitive failures and structural problems such as impediments to the parents' ability adequately to assess the costs and benefits of the information they receive.[179] Thus, information is generally substantially insufficient to reduce these risks. Cognitive abilities are required for understanding 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.[180] A clear and understandable notice on how OSPs use such information,[181] 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 their policy.[182] Any vendor of these toys must first make sure

---

[177] *See* Cass R. Sunstein, *Empirically Informed Regulation*, 78 U. CHI. L. REV. 1349, 1369 (2011) (noting that "even accurate disclosure of information may be ineffective if the information is too . . . overwhelming to be useful."); Karen Bradshaw Schulz, *Information Flooding*, 48 IND. L. REV. 755 (2015) (arguing that "information overload" could be harmful).

[178] *See* Solove, *supra* note 75, at 1883-93.

[179] As suggested by Daniel Solove, cognitive problems arise from four aspects: not reading privacy policies; not understating them; lacking enough background knowledge to make an informed choice; and choices might be skewed by various decision-making difficulties. *See id*. at 1883-93.

[180] It should be insufficient to declare that information might be shared "with third-parties" without listing who these third-parties are and what is the purpose of this information sharing. For more on the problem of vagueness, see Reidenberg et al., *supra* note 174, 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". *See* Yadron, *supra* note 139.

[181] The FTC also suggested 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. *See Children's Connected Toys*, *supra* note 45, at 2.

[182] *See* Lobosco, *supra* note 18; Steinberg, *supra* note 20. *See also Children's Connected Toys*, *supra* note 45, 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.").

that parents understand the risks, and what they are consenting to, at the point of sale.[183]

Furthermore, sellers should be obliged to place simplified and clear privacy labels on the package.[184] Beyond lucid warnings on IoToys packaging, it would be efficient to signal clearly how in these toys privacy is protected and COPPA rules are complied with. 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 organizations or the FTC, for example, like the kidSAFE Seal Program – a children's privacy certification program approved by the FTC.[185] Hello Barbie too is currently a member of such a program.[186] While not perfect, it is generally an efficient method to alert consumers to the potential risks of IoToys that do not have such a seal.[187] It could promote consumer trust, thereby persuading consumers to purchase only IoToys 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 IoToy, as their children might become secondary users. The state should therefore invest in advertisements and other forms of education

---

[183] *See Kids & the Connected Home*, *supra* note 15, at 13.

[184] *See* Lobosco, *supra* note 18; Steinberg, *supra* note 20. *See also Children's Connected Toys*, *supra* note 45, 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).

[185] 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. One of the seals is an FTC-approved COPPA certification program called "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. *See kidSAFE® Seal Program*, https://www.kidsafeseal.com/aboutourprogram.html (last visited Feb. 10, 2018).

[186] *See Official Membership Page*, KIDSAFE, http://www.kidsafeseal.com/certifiedproducts/toytalk_hellobarbie_device.html (last visited Feb. 10, 2018).

[187] Much like TRUSTe, a nonprofit organization, the first online privacy seal program in the United States. It 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 website. *See* FTC, *supra* note 77, at 6; Hertzel, *supra* note 56, at 445.

that clearly explain their potential risks. An example of such an effort that could be improved is the FBI's consumer notice for internet-connected toys, regarding the potential risks to children's privacy.[188] While important, their suggested steps are unlikely be taken by the average parent, even if exposed to them.[189] Thus, raising awareness must be more meaningful and use practical forms of communication to advise the general public on 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 entail. Exercising *verifiable parental consent* is currently promoted by COPPA.[190] Generally, this form of privacy self-management might be insufficient for IoToys.[191] The efficacy of a notice and choice mechanism has largely been contested because, inter alia, it could uninform or misinform consumers,[192] it could be impractical and ineffective,[193] and it could create undesirable externalities.[194] Generally individuals make incorrect assumptions on how their privacy is protected, and misconceive how the data is used; many lack expertise in assessing the consequences of consent.[195]

If we accept consent as a proper form of regulation, policymakers must acknowledge that in its current form it deals with IoToys insufficiently. Due to

---

[188] *See Public Service Announcement*, *supra* note 169.

[189] *See* Lori Grunin, *FBI Issues Privacy Warning for your Connected Toys*, CNET (July 18, 2017), https://www.cnet.com/news/fbi-issues-privacy-warning-for-your-connected-toys.

[190] 16 C.F.R. §§ 312.3(b), 312.5 (2012).

[191] For a comprehensive review of the efficacy of notice and choice frameworks, see Reidenberg et al., *supra* note 174, at 489-96. For criticism on the efficacy of the notice and choice mechanism to regulate information privacy, see generally Fred Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CALIF. L. REV. 1765 (2011).

[192] Users are uninformed or misinformed as they usually do not see, read or understand privacy policies. *See* Reidenberg et al., *supra* note 174, at 491.

[193] The notice and choice mechanism is considered impractical due to the amounts of privacy policies online (that might also change from time to time); that users lack knowledge of how third parties use the data; that users could not simply understand the effects of future aggregation of their data; and that users could suffer from "bounded rationality and cognitive biases." *See id.* at 492-94; Ohm, *supra* note 171, at 931.

[194] The notice and choice mechanism potentially create externalities because the disclosure of information by one individual could lead to disclosure of information of other individuals without their consent. *See* Reidenberg et al., *supra* note 174, at 495.

[195] *See* Solove, *supra* note 75, at 1885-86.

the potential risks of IoToys, regulators must require OSPs to do more than merely make reasonable efforts to obtain such consent.[196] 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 what they are consenting to.

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, whereas data is not collected from toys by default, and does so only upon enabling such option.[197] They could also reverse the choice and notice-mechanism default so that consumers will be obliged to signal their privacy preferences to the information collectors, not the reverse.[198] They could also oblige companies to offer consumers a choice between more costly services, which protect their privacy, and cheaper services, which protect it less.[199]

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.[200] While this requirement requires OSPs to collect only data that is necessary for the purposes that it is collected for, 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

---

[196] 15 U.S.C. § 6501(9) (2012).

[197] For more on the failure of opt-in consent, see Solove, *supra* note 75, at 1898.

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

[199] See, for example, in AT&T, Jon Brodkin, *AT&T Charges $29 More for Gigabit Fiber That Doesn't Watch Your Web Browsing*, ARSTECHNICA (Feb. 16, 2015, 11:38 PM) http://arstechnica.com/business/2015/02/attcharges-29-more-for-gigabit-fiber-that-doesnt-watch-your-web-browsing. This solution, however, has a social impact, as it implies that wealthy individuals deserve higher protection of privacy than non-wealthy ones. *See* Sophia Cope & Jeremy Gillula, *AT&T is Putting a Price on Privacy. That is Outrageous*, GUARDIAN (Feb. 20, 2015), https://www.theguardian.com/commentisfree/2015/feb/20/att-price-on-privacy.

[200] 15 U.S.C § 6502(b)(1)(C) (2012);16 C.F.R. § 312 (2012).

purposes" should be not qualify as fulfilling this requirement.[201] Policymakers must oblige companies to limit their data collection to what is required for the toy's core functions.[202] While it is evident that defining what these core functions are might not be easy, especially for IoToys 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.[203] Even if OSPs allow parents to change the privacy settings of IoToys, on its own this would be insufficient to mitigate IoToys risks.[204] 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."[205] This current requirement vagueness must be clarified. 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 it with any third party unless they prove full control on 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. Explaining the need for data use transparently might not be easy. OSPs might have to disclose trade secrets, and even if 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 or not. The Committee on Commerce, Science, and Transportation actually suggested (FTC) monitoring of the connected toy space and exercising authority when appropriate.[206] This oversight, however, must also be implemented carefully as it grants a state agent surveillance powers over individuals; and as history shows, these powers

---

[201] *See* ToyTalk Privacy, *supra* note 43.

[202] *See Children's Connected Toys*, *supra* note 45, at 15; Emily McReynolds et al., *Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys*, FTC (Nov. 2017) at 8, https://www.ftc.gov/system/files/documents/public_comments/2017/11/00038-141895.pdf.

[203] *Id*.

[204] While the FTC advises parents to change the privacy settings of the toy to limit the amount of personal information that is collected and transmitted, and only allow the toy collect information necessary for the toy to properly function, it might not be within the toy's options. *See Children's Connected Toys*, *supra* note 45, at 2.

[205] *See* 16 C.F.R. § 312.10 (2012).

[206] *See Children's Connected Toys*, *supra* note 45, at 15.

can be misused by the state.[207] 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.[208] The FTC's advice to parents to strengthen their passwords and frequently update the toy's software, while important, is still insufficient for data security.[209] This requirement must be clarified and recalibrated, as it does not greatly advance IoToys' 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.[210] Arguably, low security measures and data breaches could potentially result in damage to their reputation and monetary losses from fines, lawsuits or simply losing customers. The state in fact encourages parents to respond actively to IoToys' security measures. The FTC advises them to examine companies' prior history of security breaches.[211] The FBI has further recommended that parents examine the toy's internet and device-connection security measures and probe any known security issues; use toys in environments with trusted and secured Wi-Fi internet access; research where user data is stored and whether any publicly available reporting exists regarding their reputation and stance on cyber security; and ensure the toy is turned off when not in use.[212]

Prima facie, IoToys manufacturers and OSPs would wish to invest in measures to protect from harm their products and services, their reputation and share price, and their customers. As this market-based approach suggests, with

---

[207] For more on surveillance the digital age, *see generally* BRUCE SCHNEIER, 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 (2017).

[208] 16 C.F.R. § 312.3(e) (2012).

[209] *See Children's Connected Toys*, *supra* note 45, at 2.

[210] 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 generally* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS (Sálvio Marcelo Soares ed., 2007) (1776).

[211] *See Children's Connected Toys*, *supra* note 45, at 2.

[212] *See Public Service Announcement*, *supra* note 169.

proper incentives, the modality of law is not needed—absent substantial market failures 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,[213] 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 we add regulatory requirements of disclosure like security standards or data breach notifications[214] to reduce information gaps—commonly termed the *regulation through disclosure* approach[215]—this will not necessarily lead to a market response.[216] It might be too vague for consumers to fully understand or simply not be fully comprehensible without substantial expertise in cybersecurity and the aforementioned cognitive bias.

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.[217] Notably, however, IoToys are certainly not a necessity,

---

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

[214] 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).

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

[216] *See, e.g.*, Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256, 264 (2011). 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).

[217] *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.").

and parents' discontent could be realized simply by their not purchasing any IoToy.

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 children. Policymakers must set a higher threshold than "reasonable" and demand that toy manufacturers and OSPs comply with high security standards for the IoToy 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;[218] use strong encryption standards; and actively update security measures.[219] The FTC has in fact suggested that toymakers be obliged to build-in effective security from the start.[220] The FTC 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 be incentivized to implement anonymization measures,[221] differential privacy[222] and any other Privacy

[218] ToyTalk, for instance, currently offers a monetary bounty for reports of qualifying security vulnerabilities. *See ToyTalk*, HACKERONE, https://hackerone.com/toytalk (last visited Feb. 10, 2018).

[219] *See Kids & the Connected Home*, *supra* note 15, at 15; *Children's Connected Toys*, *supra* note 45, at 2.

[220] *See Children's Connected Toys*, *supra* note 45, at 15.

[221] 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 highly difficult. Notably, at least one IoToys' OSP declare that they anonymize the data and further ensure it's stored in multiple different places. *See* Sara Sorcher, *The Internet of Toys raises new Privacy and Security Concerns for Families*, CS MONITOR (July 22, 2016), https://www.csmonitor.com/World/Passcode/2016/0722/The-Internet-of-Toys-raises-new-privacy-and-security-concerns-for-families.

[222] Differential privacy relates to a method by which noise is added systematically to results of data quarries, while no single person's inclusion or exclusion from the database can affect the results of queries dramatically. Using differential privacy correctly should assure that no user could infer anything about another user. For an analysis and critique of differential

Enhancing Technologies (PETs) tools,[223] as long as the FTC can verify their applicability to safeguarding children's privacy.

5. *Effective Enforcement*

The FTC's option to sanction COPPA violation is in itself insufficient to be considered effective enforcement.[224] 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.[225] Even without adhering to direct oversight, at the very least the FTC must investigate and rectify instances where reporters show that an IoToy is not secure enough.[226] 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.[227]

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;[228] nonetheless the FTC should exercise its

---

privacy, see Jane Bambauer, Krishnamurty Muralidhar & Rathindra Sarathy, *Fool's Gold: An Illustrated Critique of Differential Privacy*, 16 VAND. J. ENT. & TECH. L. 701 (2014).

[223] *See supra* note 147.

[224] This fifth requirement was further acknowledged by the FTC as a critical component to protect privacy online. *See* FTC, *supra* note 77, at i.

[225] *See Electronic Toy Maker VTech Settles FTC Allegations that it Violated Children's Privacy Law and the FTC Act*, *supra* note 141.

[226] Research showed that there is a high rate of potential COPPA violations in Apps that are directed to children, while pointing out to troubling lack of oversight. *See* Serge Egelman, *We Tested apps for Children. Half Failed to Protect their Data*, WASH. POST (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. *See also supra* notes 139-140.

[227] *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.

[228] Generally speaking, deterrence theory had 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).

vested powers of enforcement to impose the highest fines possible.[229] Sanctioning companies like VTech to the tune of $650,000 for a substantive data breach is unlikely to advance the deterrence rationale, considering their $689.4 million gross profits that year.[230] OSPs must not see fines as costs of doing business, and should reflect further on the gravity of poor security measures. Policymakers should thus implant in the FTC substantial regulatory teeth. This would enable the Commission's fines not merely to reflect the level of consumer loss, but rather violations, with fines as percentages of annual global turnover.[231] 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.[232]

*

Legal intervention is thus greatly needed to secure informational privacy of children better in the IoToys market. COPPA regulation must frequently be updated to better address the risks that IoToys entail, and frequently revisited in view of technological changes that could affect the risks in these toys. For example, the future IoToy 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.

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 be acknowledged. If an IoToy increases the risks to children's privacy, parents must also become more involved in safeguarding their children. Their involvement, however, should not be treated lightly as it bears on important normative questions that must be

[229] 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 million. *See* Solove & Hartzog, *supra* note 70, at 605, 647.

[230] *See Annual Report 2017*, VTECH HOLDING LIMITED, at 6 (2007), https://www.vtech.com/wp-content/uploads/2017/06/AR2017_eng.pdf.

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

[232] *See* Solove & Hartzog, *supra* note 70, at 600 (noting that the FTC's staff devoted to privacy issues is relatively small).

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?[233] More particularly, should children's right to privacy be viewed only as a right from third-parties, or also from their parents? In other words, how can we ensure children's privacy outside their household but also not completely abolish it within what they view as their safe place?

IV. TAKING CHILDREN'S PRIVACY SERIOUSLY

Parents have the responsibility to safeguard their offspring from dangers. They must make decisions regarding various aspects of their lives, especially their health, development and safety. To do so, they might oblige them, inter alia, to wear helmets and kneepads when riding their bicycles, sit in car seats, and only play in safe playgrounds.[234] They might also become closely involved in their lives and even use sensors and monitors to assure their safety. While parents might always have been involved in their children's lives to some extent, researchers have witnessed an increase 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.[235] Essentially, children today are probably the most watched-over generation in history.[236]

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

---

[233] *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. 765, 766 (2017) (discussing the 'empowerment vs protection' dilemma in child rights debates).

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

[235] 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. It had also been characterized, inter alia, as invasive parenting; overparenting; aggressive parenting; modem parenting; and snowplow patents. *See* Kathleen Vinson, *Hovering Too Close: The Ramifications of Helicopter Parenting in Higher Education*, 29 GA. ST .U. L. REV. 423, 424 (2013); Bernstein & Triger, *supra* note 234, at 1225; Lisa Belkin, *Let the Kid Be*, N.Y. TIMES, May 31, 2009, at MM19.

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

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.[237] It also further seeks to discuss the *privacy protection paradox*,[238] 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.

A. Parenting in the IoToys Era

Parenting generally involves a balance of risk management.[239] Many parents might view good or responsible parenting as being all-knowing, which requires them to monitor their behavior.[240] They might monitor their children even before their birth, using ultrasound screening to detect fetal anomalies and see their unborn baby's movements and hear its sounds.[241] 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.[242] They might even monitor their child when another caregiver is present by using, inter alia, cameras hidden inside another object ("nanny cams").[243] When their children are old enough to interact with the digital world, parents might monitor their conduct by various methods. Parents' consent to their using the internet, for instance, might rely on imposing rules and restrictions such as placing the computer in a shared space[244] or obliging their children to share the content of their conversations and even their usernames and passwords with them.[245] They might also embrace social approaches like educating them to share what they

---

[237] *See* Macenaite, *supra* note 233, at 766-67.

[238] *See The Protection of Children Online*, *supra* note 40.

[239] *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).

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

[241] *See* Bernstein & Triger, *supra* note 234, at 1232; Deborah Lupton & Ben Williamson, *The Datafied Child: The Dataveillance of Children and Implications for their Rights*, 19 NEW MEDIA & SOC. 780, 783-84 (2017).

[242] *See generally* Margaret K. Nelson, *Watching Children: Describing the Use of Baby Monitors on Epinions.com*, 29 J. FAM. ISSUES 516 (2008); Bernstein & Triger, *supra* note 234, at 1232-33; Lupton & Williamson, *supra* note 241, at 783-84.

[243] *Id*.

[244] *See* BOYD, *supra* note 240, at 72.

[245] *Id*. at 72-73.

are doing, or by using technical tools like monitoring software.[246] Essentially, many parents will attempt to strengthen their control and track almost everything their children do offline and online.[247]

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. Parents might fear that their children's data will be misused, but also be alert to their exposure to harmful content, cyberbullying and inappropriate contact. These fears might be further enhanced as their children's interactions could be perceived as less visible to them than in the kinetic world. Under this assumption, parents will use technology to monitor their children online as a responsive measure against the risks of technology.

While parents' mediation is effective in reducing online risks to their children is disputable,[248] these fears are non-fictional, 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 their control over their play because of these risks and the invisibility of their actions from their point of view. COPPA regulation deals directly with the protection of children's privacy from misuse of their data by third parties. 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.[249]

Some OSPs took the right of parental review a step farther in IoToys, by providing parents real-time access to their children's recordings.[250] In some instances they could even be notified when a new recording was made.[251] At

---

[246] *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).

[247] *See* BOYD, *supra* note 240, at 70-72.

[248] For an empirical work on reducing online risks by parental mediation *see, e.g.,* Sonia Livingstone & Ellen J. Helsper, *Parental Mediation and Children's Internet Use*, 52 J. BROADCAST ELECTRON. MEDIA 581 (2008); Häkan Stattin & Margaret Kerr, *Parental monitoring: A reinterpretation*, 71 CHILD DEVELOPMENT 1072 (2000); Caitlin Elsaessera , Beth Russellb, Christine McCauley Ohannessianc & Desmond Patton, *Parenting in a digital age: A review of parents' role in preventing adolescent cyberbullying*, 35 AGGRESSION & VIOLENT BEHAVIOR 62 (2017).

[249] 15 U.S.C. § 6502 (2012); 16 C.F.R. § 312.6(a)(3) (2012).

[250] *See* ToyTalk Privacy, *supra* note 43 ("You may review and delete account information and Recordings that are in your parent account via the Settings page when you log in to ToyTalk's website. To review or delete Recordings, click on "View Conversation Data.").

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

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.[252] However, this form of monitoring is troubling from a privacy perspective.

While supposedly COPPA regulation increases children's privacy by strengthening parents' control over the sensitivity of disclosed information, it might further jeopardize children's privacy from a different perspective: the children's. Due to the characteristics of many IoToys, children might become convinced that the IoToy is their best friend—even anthropomorphize it—and consequently share their deepest secrets with it.[253] Perhaps obviously, the regulatory framework does not deem such secrets sensitive information per se as safeguarding this information from third parties might not seem important. Its proclaimed non-sensitive nature could be further learned from practices of OSPs that sometimes make it easy for parents to share IoToys' recordings through social media like Facebook, YouTube and Twitter.[254] From the children's perspective, however, their secrets are probably the most valuable privacy rights they own.[255]

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,[256] 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. 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 them as surveillance officers, and normalizes such

---

[252] *See Public Service Announcement*, *supra* note 169.

[253] *See supra* part III.A.

[254] *See Privacy Policy*, TOYTALK (last revised Apr. 11, 2017), https://www.toytalk.com/legal/privacy.

[255] *See infra* part IV.B.

[256] It is notable that COPPA was partially designed to enhance parental involvement in a child's online activities. This, however, is not the rational 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; to maintain the security of children's personal information collected online; and to limit the collection of personal information from children without parental consent. *See* 144 Cong. Rec. S12741 (Oct. 7, 1998) (statement of Sen. Bryan).

conduct for both the parents and their children—when they will 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 constant monitoring of children's privacy? Should children possess the right to privacy from their parents? They 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 their lives like infanthood, this might be less evident as they lack a "theory of mind," namely are unable to distinguish self from other.[257] But from that point, approximately at age four,[258] children learn that they can keep secrets from their parents.[259] That is when the potentially negative effect of ubiquitous surveillance begins.

The world's perception of children has been the subject of many scholarly debates, from Jean Piaget's development stages and process to Donald Winnicott's monumental work on stages of child development and practice of childhood play.[260] A key example is Erik Erikson's work, which stresses the importance of the years from middle childhood (approximately ages 6 to 10) to early adolescence (approximately ages 11 to 14) for children's development. Erikson argued, inter alia, that these stages are important for

---

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

[258] *See* Beate Sodian et al., *Early Deception and the Child's Theory of Mind: False Trails and Genuine Markers*, 62 CHILD DEV. 468 (1992).

[259] *See generally* Malinda J. Colwell et al., *Secret Keepers: Children's Theory of Mind and their Conception of Secrecy*, 186 EARLY CHILD DEVELOPMENT & CARE 369 (2016); Heinz Wimmer & Josef Perner, *Beliefs about Beliefs: Representation and Constraining Function of Wrong Beliefs in Young Children's Understanding of Deception*, 13 COGNITION 103 (1983).

[260] *See generally* JEAN PIAGET, THE CHILD'S CONCEPTION OF THE WORLD (1926); DONALD WINNICOTT, THE CHILD AND THE FAMILY (London: Tavistock, 1957); DONALD WINNICOTT, THE CHILD THE FAMILY AND THE OUTSIDE WORLD (London: Pelican Books, 1964); DONALD WINNICOTT, THE FAMILY AND INDIVIDUAL DEVELOPMENT (London: Tavistock, 1965). For an excellent summery on children's perception of the right to privacy *see generally* Sunny Kalev, *"I Decide for Myself" – Children's Privacy in the Digital Age and the Right to Withdraw from Parental Consent*, 41 IYUNEY MISHPAT – TEL AVIV U. L. REV. (forthcoming, 2018) [Hebrew].

developing a sense of self-esteem and individuality.[261] Within these psychological assessments, play itself is also is an important part of how children learn about the world, and parents' intrusion could fulfill an integral role within play.[262] 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.[263] More closely 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 their children's privacy should be protected by them. 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.[264] Arguably, the perceived risks of the digital world do not change the scope of this prerogative, they indeed even intensify its need. By this approach, parents must be in greater control, especially in the digital world.[265]

From a legal perspective, parents are not normally prohibited from recording their children or even reading their secret diary.[266] Parents' fundamental right to make decisions regarding the "care, custody, and control of their children" is even protected by the Due Process Clause of the Fourteenth Amendment.[267] They decide what is best for their children, and whether or not they should be aware that any conversation they hold be

---

[261] *See generally* ERIK H. ERIKSON, CHILDHOOD AND SOCIETY (New York: Norton, 1963); Jacquelynne S. Eccles, *The Development of Children Ages 6 to 14*, 9 THE FUTURE OF CHILDREN 30, 32-34 (1999).

[262] *See* Emmeline Taylor & Katina Michael, *Smart Toys that are the Stuff of Nightmares*, 35 IEEE 8, 9 (2016).

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

[264] *Id*. at 488.

[265] *See* Antigone Davis, *Hard Questions: So Your Kids Are Online, But Will They Be Alright?*, FBNEWSROOM (Dec. 4, 2017), https://newsroom.fb.com/news/2017/12/hard-questions-kids-online ("Parents 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.").

[266] *See* Kay Mathiesen, *The Internet, Children, and Privacy: The Case against Parental Monitoring*, 15 ETHICS & INFO. TECH. 263, 265 (2013).

[267] *See* U.S. CONST. amend. XIV. For the Supreme Court ruling on parents' discretion over their own children, see Troxel v. Granville, 530 U.S. 57 (2000). For further information on the history of parental autonomy in common law jurisdictions, see Francis Barry McCarthy, *The Confused Constitutional Status and Meaning of Parental Rights*, 22 GA. L. REV. 975 (1988).

accessible to them. Under some circumstances they could even be immune to tort liability under the parental immunity doctrine.[268] As a result, children do not possess the right to conceal information from their parents.[269] Troubling in COPPA regulation is not that parents are generally entitled to spy on their children, but that the regulatory framework encourages OSPs to furnish such measures. When parent buys their children an IoToy that is supposedly their new best friend, they will not suspect that their parents can eavesdrop on every conversation they have with the doll.

Equally troubling is that parents' depriving their children of their privacy is becoming more invisible to them 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.[270] They might 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 it 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

---

[268] 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, e.g., 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 (2014); Pimentel, *supra* note 239, 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, e.g., Maureen S. Binetti, *Child's Right to Life, Liberty and the Pursuit of Happiness: Suits by Children Against Parents for Abuse and Abandonment*, 34 RUTGERS L. REV. 154 (1981).

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

[270] A fairly known example of behavioral shaping by surveillance is a toy that is based on the Christmas book "Elf on the Shelf". In their book, Carol Aebersold and Chanda Bell describe a minion of Santa who spies on children. Based on the book, a doll which carries the name of its title was put on sale for parents, teaching children to alter their behavior when been "watched" by the elf. For more on the privacy implications of the "Elf on the Shelf", see Laura E. Pinto & Selena Nemorin, *Normalizing Panoptic Surveillance among Children: 'The Elf on the Shelf'*, 24 OUR SCHOOLS/OUR SELVES 53 (2015); Alex Steed, *No to 'Elf on the Shelf': Christmas Shouldn't be an Extension of our Surveillance Culture*, BDN (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.

monitoring are mostly invisible to adults too, and perhaps these mechanisms actually better prepare children for the "real world."[271] This notion augments a well-known idiom on the demise of privacy in the digital age.[272] 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.[273] They simply view it differently from adults.[274] For instance, they could view it simply as "aloneness,"[275] "to hide secrets or special things," "to keep things to yourself" or "not to talk to strangers."[276] They might value privacy as an enabler tool "to engage in identity play, seek advice, form relationships, and immerse themselves in peer communication."[277] When they experience constant surveillance by their parents, this shapes their understanding of privacy and limits their ability to make independent choices.[278] It becomes even more important when their lives are already largely

[271] For more on the invisibility of data collection and privacy, see Saadi Lahlou, Marc Langheinrich & Carsten Röcker, *Privacy and Trust Issues with Invisible Computers*, 48 COMM. ACM 59 (2005).

[272] Many argue that privacy is dead or at least, that it deserves minimal protection in digital age at best, and that even if privacy still exists it is merely a tradeable currency. Scott McNealy, chief executive officer of Sun Microsystems, is famously quoted suggesting "You have zero privacy anyway . . . Get over it." *See* Polly Sprenger, *Sun on Privacy: 'Get Over it'*, WIRED (Jan. 26, 1999), https://www.wired.com/1999/01/sun-on-privacy-get-over-it. *See also* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1462 (2000). 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 (2007).

[273] *See generally* BOYD, *supra* note 240, at 53-54.

[274] *See, e.g.*, Sonia Livingston, *Children's Privacy Online: Experimenting with Boundaries Within and Beyond the Family*, *in* COMPUTERS, PHONES, AND THE INTERNET: DOMESTICATING INFORMATION TECHNOLOGIES 145, 152 (R. Kraut, M. Brynin, & Kiesler, Sara, eds. 2006) ("Children seek privacy, but as a means to an end not an end in itself.").

[275] *See* Melton, *supra* note 263, at 488. They might also view privacy as "being alone, managing information, being unbothered, and controlling access to places". *See generally* Maxine Wolfe, *Childhood and Privacy*, *in* CHILDREN AND THE ENVIRONMENT 175 (I. Altman and J.F. Wohlwill eds., 1978).

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

[277] *See* Priya Kumar et al., *'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online*, 1 PACM HUMAN-COMPUTER INTERACTION 64, 64:2 (2017); Livingston, *supra* note 274, at 152.

[278] *See* BOYD, *supra* note 240, at 73.

monitored by their parents,[279] and further strengthens the traditional power structure of the "all-knowing" adult over the "all-learning" child.[280]

Parents should be generally aware of what their children do with IoToys, but this should also be balanced properly by the child's right to privacy.[281] 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 for them. They might not even care if OSPs mine their data or use it for various purposes. That is why their parents are tasked to consent on their behalf. But being unaware that IoToys record their conversations,[282] and that their parents have access to them, might change their attitude to their parents upon discovering their monitoring and the meaning of privacy.

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, while enjoying a constitutional right, 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 and safety concerns arise.[283] The state could in fact triumph over parental autonomy under some circumstances by regulating the parent-child relationship.[284] 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.[285]

---

[279] *Id*. at 75 ("Privacy is especially important for those who are marginalized or lack privilege within society.").

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

[281] *See* de Haan, *supra* note 246, at 194 ("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.

[282] *See* McReynolds et al., *supra* note 202, at 2.

[283] *See, e.g.*, Elizabeth G. Porter, *Tort Liability in the Age of the Helicopter Parent*, 64 ALA. L. REV. 533 (2013).

[284] *See* Elaine M. Chiu, *The Culture Differential in Parental Autonomy*, 41 U.C. DAVIS L. REV. 1773, 1986-90 (2008).

[285] 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).

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, it must not further foster its violation by granting parents' better tools to violate their privacy. It must not designed parents as surveillance officers. The parent-child dimension should be further addressed by policymakers within the notions of notice and consent. By doing so, they will 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. Even if such delicate regulation takes place, COPPA might not be the right venue for it. Still, regulators should at least acknowledge children's privacy interests, in contrast to the concept of privacy as portrayed by their parents. Not only does COPPA not take into account children's view of privacy, it indeed enhances its violation, 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.[286]

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 by means of other factors. The parent-child relationship should not be set aside, and children's trust in their parents should be taken seriously.[287] Involving children in IoToys decisions could benefit their technological education and improve the parent-child relationship, and the understanding of privacy by both sides.[288] Increasing

---

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

[287] *See* Davis, *supra* note 265; Meg Leta Jones & Kevin Meurer, *Can (and Should) Hello Barbie Keep a Secret?*, IEEE ETHICS (2016).

[288] *See, e.g.*, Yasmeen Hashish, Andrea Bunt & James E. Young, *Involving Children in Content Control: A Collaborative and Education-Oriented Content Filtering Approach*, PROC. CHI. ACM 1797 (2014).

children's participatory rights by viewing this as a positive liberty[289] could enhance children's liberty and provide considerable privacy protection toward their attaining independence.[290]

Raising children's' awareness of the IoToy's ability to share their data with their parents should not be generally contested. There is no rationale behind knowing their secrets per se—such knowledge is meant only to safeguard them from revealing personal information that could be misused. Parents could achieve this purpose simply by listening to the communication from the IoToy—without hearing their child's answer.[291] Also, children must be made aware of the practical—not merely abstract—risks of telling their IoToy everything. So to ensure their 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.[292] The participants could together decide, for instance, how to adjust the IoToy'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 IoToy throughout its use, but more especially in the toy's first communication with the 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.[293]

Other regulatory ways of raising awareness could be achieved by investing in informative state-sponsored advertisements directed at children, or obliging toy manufacturers or OSPs of IoToys to include these data in their

---

[289] Under a negative liberty approach, privacy should be viewed as a form of exercising personal choice. *See* Cohen, *supra* note 160, at 1907.

[290] 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 160, at 1907.

[291] *See* Leta Jones & Meurer, *supra* note 287 ("ToyTalk could display Barbie's side of the conversation to parents without revealing their child's responses.").

[292] 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.

[293] *See* McReynolds et al., *supra* note 202, at 8.

advertisements. Thereafter the state could also invest in more general awareness-raising campaigns or even promote awareness through the education system.[294] 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 *duel-consent requirement* could IoToys be activated. Using 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;[295] but in the context of privacy and IoToys they should at least have the right to roll back the invisible boundaries of parental surveillance.

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, it is not even merely a right to privacy or a right to be left alone, but simply the freedom to play with toys, without realizing that it is actually their parents who are toying with their privacy. It is a liberty simply to be themselves. To mitigate properly the privacy risks that IoToys entail, 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 their autonomy. COPPA regulation must therefore be revisited and recalibrated to properly meet the challenges of IoToys. This Article suggested such a form of recalibration by revisiting COPPA's requirements and adjusting them to IoToys. It suggested 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 them 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

---

[294] *See* de Haan, *supra* note 246, at 194 ("Parental mediation might be stimulated by awareness-raising campaigns or by meetings at schools.").

[295] For a discussion on the possession of rights by minors in the U.S., 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).

argue that any attempt to safeguard children's privacy in a society racing into a ubiquitous surveillance era might 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 necessitate 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.