THE INTERNET OF CHILDREN: PROTECTING CHILDREN'S PRIVACY IN A HYPER-CONNECTED WORLD

Eldar Haber[*]

Children's privacy is at great risk. Due to the emergence of the Internet of Things ("IoT"), whereby ordinary objects became connected to the internet, children might now be constantly datafied during their daily routines, with or without their knowledge. IoT devices might collect and retain mass amounts of data and metadata on children and share them with various parties—able to extract data on where children are, what they are doing or saying, and perhaps even capture imagery and videos of them. While Congress previously responded to rather similar privacy threats that emerged from the internet with the enactment of the Children's Online Privacy Protection Act ("COPPA"), this regulatory framework only applies to a limited set of IoT devices—excluding those which are not directed towards children nor knowingly collect personal information from them. Essentially, COPPA is ill-suited to properly safeguard children from the privacy risks that IoT entails, as it does not govern many IoT devices that they are exposed to. The move towards an "always-on" era, by which many IoT devices constantly collect data from users, regardless of their age, exposes them to great privacy risks. The dire consequences that IoT entails for children's privacy thus necessitates a comprehensive reform of the regulatory framework that governs such protection.

This Article focuses on the privacy implications of IoT on children under the current regulatory framework, analyzes its shortcomings to protect them, and offers various solutions to properly safeguard children in a hyper-connected world. It proceeds as follows: The second Part surveys surveillance and the development of IoT within digital datamining practices. This Part then turns to discuss the potential interaction of children with IoT devices while offering a taxonomy of different types of IoT devices. Part III turns to discuss IoT in the context of children's privacy. It begins with a general review of children's right to privacy in general and the regulatory framework that governs it online. This Part then discusses said regulatory

[*] Senior Lecturer, Faculty of Law, University of Haifa; Visiting Professor, Bocconi University, Italy; Faculty member, Center for Cyber, Law and Policy (CCLP), and Haifa Center for Law and Technology (HCLT), University of Haifa. I am much grateful to Gabriel Focshaner, Naama Shiran and Tal Tamches for their excellent assistance in research. This research was supported by a Grant from the GIF, the German-Israeli Foundation for Scientific Research and Development.

framework in light of IoT and suggests that merely recalibrating this framework might not advance children's privacy protection to a great extent. Part IV further challenges the current regulatory framework set to protect children online. It begins with questioning the sectoral approach to privacy in general; adds non-legal modalities like the market, social norms, and technology to aid in such protection; and raises dilemmas on digital parenting and the future of children's privacy in the always-on era. The final Part summarizes the discussion and suggests that the always-on era must not lead to the demise of privacy in general, and especially, that of children.

TABLE OF CONTENTS

I. INTRODUCTION

We live in a society that is subject to constant surveillance and datafication by private and governmental entities alike. Almost everything end users do on computerized networks is known to private parties.[1] The emergence of what is known as the *Internet of Things* ("IoT")[2]—whereby ordinary objects became connected to the internet—further expanded the datamining and surveillance capabilities of many private entities. Smart TVs, wearables, computerized personal assistants, and even ordinary household devices like washing machines, toasters, and refrigerators can collect and retain mass amounts of data and metadata on their users and share this data with various parties.[3] They might be able to extract data on where their users are, what they are doing or saying, and perhaps even capture imagery and videos of them. Surveillance literally surrounds us as we enter a world awash with sensors.[4]

1. *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002).

2. The term 'Internet of Things' is attributed to Kevin Ashton. *See* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), http://www.rfidjournal.com/that-internet-of-things-thing.

3. Vivek Wadhwa, *When the Toaster Shares Your Data with the Refrigerator, the Bathroom Scale, and Tech Firms*, SINGULARITYHUB (June 30, 2015), https://singularityhub.com/2015/06/30/when-the-toaster-shares-your-data-with-the-refrigerator-the-bathroom-scale-and-tech-firms/.

4. *See infra* Part I.

Here enters the *Internet of Children*. Children are generally first exposed to technology at very early stages of their lives, many times even prior to birth.[5] Their exposure to IoT might begin at early stages of their development, from IoT-based sensors, monitors, and wearables, to actively playing with IoT toys or devices like those of Hello Barbie or My Friend Cayla.[6] Along with such use of technology, children could also be exposed to various types of IoT devices in their daily environments, many times inadvertently. They might be surrounded by smart devices like TVs, computerized personal assistants, and many other IoT-based devices that might collect data on them constantly. Thus, it would be highly difficult for children to avoid surveillance and datafication in this era.

While IoT could have many benefits, the constant interaction with it, especially when it occurs inadvertently, poses many threats to children. These devices could be misused to inappropriately contact children, expose them to harmful content, and in some scenarios, even lead to mental and bodily harm.[7] Aside from these threats, society's push towards an ubiquitous surveillance era affects children's notions of liberty and negatively affects their fundamental right to privacy. Policy-makers in fact already acknowledged the potential risks to privacy by the internet back in 1998, while crafting the Children's Online Privacy Protection Act ("COPPA") to protect them.[8] But the rapid pace of technological developments and innovation has led to applying the regulatory framework that governs internet websites only to IoT toys ("IoToys") and devices that are targeted at children. Aside from potential criticism on the applicability of this framework to properly regulate the datafication from IoToys and other IoT devices, it generally fails to include devices that do not fall under COPPA terms, meaning that it does not govern many other IoT devices that children are exposed to during their daily routines.

And much like they do with adults, IoT devices collect information on children and transmit it over the internet, enabling service providers to retain it for indefinite periods, to be used for various purposes.[9] These devices, which currently fall outside the scope of the regulatory framework set to protect children, could be equipped with many sensors that could capture the voices, conversations, locations, and even imagery of anyone within their vicinity. Some devices even operate constantly, *i.e.*, they are "always-on," meaning that many children will be datafied as they go along their daily routines, while COPPA will generally not apply to such datamining practices. Thus, as IoT devices could pose dire consequences for the protection of young children's privacy in the always-on era, the regulatory framework that governs such protection should be reevaluated, and perhaps forsaken entirely, in light of these new privacy threats.

5. *Id.*

6. *See infra* Section II.B.

7. *See infra* note 76.

8. *See* Children's Online Privacy Protection Act (COPPA), Pub. L. No. 106–70, 112 Stat. 2681 (1998) (codified as amended at 15 U.S.C. §§ 6501–06 (2018)). For further information on COPPA and the regulation that supplements it, see *infra* Section III.A.

9. Marie-Helen Maras, *4 Ways "Internet of Things" Toys Endanger Children*, SCI. AM.: TECH (May 10, 2018), https://www.scientificamerican.com/article/4-ways-internet-of-things-toys-endanger-children/.

This Article focuses on the privacy implications of IoT on children under the current regulatory framework, analyzes its challenges to protect them, and offers various solutions to properly safeguard children in the always-on era. It proceeds as follows: The second Part surveys digital surveillance and the development of IoT within datamining practices. That Part then turns to discuss the potential interaction of children with IoT devices while offering a taxonomy of different types of IoT devices. Part III turns to discuss IoT in the context of children's privacy. It begins with a general review of children's right to privacy and the regulatory framework that governs it online. That Part then discusses such regulatory framework in light of IoT and suggests that merely recalibrating this framework might not advance children's privacy protection to a great extent. Part IV further challenges the current regulatory framework set to protect children online. It begins with questioning the sectoral approach to privacy in general; adds non-legal modalities like the market, social norms, and technology to aid in such protection; and raises dilemmas on digital parenting and the future of children's privacy in the always-on era. The final Part summarizes the discussion and suggests that the always-on era must not lead to the demise of privacy in general, and especially, that of children.

II. CHILDREN IN A HYPERCONNECTED WORLD

The possibilities of connecting to external computer networks became almost endless for individuals in modern society in the twenty-first century. Technological developments enabled many individuals to be constantly connected to the internet via traditional computers, mobile phones, and tablets, to name but a few examples. In the past few years, this form of accessibility has moved far beyond traditional computers through what is commonly termed as the *Internet of Things*.[10] Within this technological innovation, almost any ordinary object could connect to the internet, constantly collecting and retaining data.

Much like adults, children are not generally excluded from this modern era. They might use computers and smartphones that are connected to the internet, wear wearable devices, and even play with toys or use devices that are designed for their use. But other than specific toys or devices that are targeted at children, presumably purchased and configured by their caregivers—thus generally within their basic discretion on how to expose them to digital technology—some devices are increasingly becoming embedded into their parents' daily lives, and subsequently, the children's lives. It thus might become inevitable for children to make use of many IoT devices—subjecting them to be online almost constantly. As this Part further argues, children's interaction with IoT, whether directly or indirectly, exposes them to various risks and to almost constant datafication and surveillance.

10. *See* Matt Burgess, *What Is the Internet of Things? WIRED Explains*, WIRED (Feb. 16, 2018), http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot; Ashton, *supra* note 2.

A. Digital Surveillance and Datafication in IoT

Surveillance preceded technology. It is probably almost as old as civilization itself.[11] While the kinetic world had placed some barriers on the ability to conduct surveillance, technological developments have made it easier.[12] These developments aided in reshaping and broadening the potential scope of surveillance. The telescope, for instance, enhanced the ability to gather and collect information for whoever desired to spy.[13] When technology continued to evolve, surveillance capabilities expanded accordingly. Communications media like that of telegraph, paper mail, and telephone subjected individuals to potential surveillance by various entities.[14] Essentially, when communication between individuals involved third parties, like that of the postal service and telephone operators, the potential risk that the transferred data could be compromised arose.

One of the biggest leaps thus far in datamining capabilities resulted from digital technology and, perhaps mainly, the internet. The internet made it difficult to avoid at least some form of surveillance in the twenty-first century. It enabled private entities to mine data and acquire knowledge of what many individuals are doing at almost any given time.[15] Online intermediaries were placed in a position that enabled them to exercise control over content, access, distribution channels, and end users' personal data and devices.[16] Mobile phone companies and online service providers, for instance, gather mass amounts of data and metadata on their users and their behavior.[17] The internet has also enabled the collection and retention of data on users' interests, consumption habits, opinions, and tastes.[18]

The internet was merely the beginning in the context of datamining and control. IoT devices could potentially acquire and transmit both metadata and data on their users and thus they naturally expand data gathering and surveillance capabilities.[19] IoT increases tracking powers of individuals' homes, vehicles,

11. *See generally* KEITH LAIDLER, SURVEILLANCE UNLIMITED: HOW WE'VE BECOME THE MOST WATCHED PEOPLE ON EARTH (2008).

12. *See* discussion *infra* Section II.A.

13. For more on the history of the telescope, see Christopher McFadden, *A Brief History of the Telescope: From 1608 to Gamma-Rays*, INTERESTING ENGINEERING: SCIENCE (May 27, 2018), https://interestingengineering.com/a-brief-history-of-the-telescope-from-1608-to-gamma-rays.

14. *See* Berger v. New York, 388 U.S. 41, 45–46 (1967).

15. *See* Niva Elkin-Koren & Eldar Haber, G*overnance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105, 113 (2016); Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 262–70 (2008); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 353 (2008); Solove, *supra* note 1, at 1084. For more on surveillance in the digital age, see generally BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015).

16. *See* Elkin-Koren & Haber, *supra* note 15, at 113.

17. Almost everything end-users do on computerized networks is known to private parties. *See, e.g.*, Solove, *supra* note 1, at 1084.

18. *See* Elkin-Koren & Haber, *supra* note 15, at 113.

19. *See* discussion *infra* Section II.A.

and bodies.[20] It greatly increases the datafication abilities of intermediaries, as IoT devices could be equipped with various sensors, like microphones and cameras. Smart TVs could obtain watching habits,[21] and might capture voice recordings of their users.[22] Smartphones enable datamining by various service providers, like network, hardware, and software providers.[23] Wearable IoT devices might monitor body activity and vital signs, such as heart rate, number of steps taken, sleeping patterns, and location, among other things.[24] Computerized personal assistants like Amazon Echo or Google Home operate in an always-ready mode, *i.e.*, they will record any data following an activation command,[25] while

20. *See, e.g.*, Julia Powles, *Internet of Things: The Greatest Mass Surveillance Infrastructure Ever?*, GUARDIAN (July 15, 2015, 10:10 AM), https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance.

21. *See* Chris Hoffman, *How to Stop Your Smart TV from Spying on You*, HOW-TO GEEK (Nov. 16, 2015, 6:40 AM), http://www.howtogeek.com/233742/how-to-stop-your-smart-tv-from-spying-on-you.

22. *See* Darren Orf, *Samsung's SmartTV Privacy Policy Raises Accusations of Digital Spying*, GIZMODO (Feb. 8, 2015, 2:30 PM), https://gizmodo.com/samsungs-smart-tv-privacy-policy-raises-accusations-of-16845 34051; Letter from EPIC to the Attorney General and the FTC Chairwoman 3 (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf ("When the voice recognition feature is enabled, everything a user says in front of the Samsung SmartTV is recorded and transmitted over the Internet to a third party regardless of whether it is related to the provision of the service.").

23. *See, e.g.*, Neil McAllister, *How Many Mobile Apps Collect Data on Users? Oh . . . Nearly All of Them*, REGISTER: SECURITY (Feb. 21, 2014, 2:28 AM), http://www.theregister.co.uk/2014/02/21/appthority_app_privacy_study.

24. Fitbit, for instance, is a fitness tracker that monitors steps and could provide insights, *inter alia*, on an individual's heart rate or quality of sleep. *See* Andrew Hilts et al., *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, OPEN EFFECT REPORT 3–6 (2016), https://openeffect.ca/reports/Every_Step_You_Fake.pdf. For a taxonomy of personal health monitors, see Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98–99 (2014).

25. 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. All you have to do is ask. Echo has seven microphones and beam forming technology so it can hear you from across the room—even while music is playing. Echo is also an expertly tuned speaker that can fill any room with 360° immersive sound. When you want to use Echo, just say the wake word 'Alexa' and Echo responds instantly. If you have more than one Echo or Echo Dot, Alexa responds intelligently from the Echo you're closest to with ESP (Echo Spatial Perception)." *See Amazon Echo – Black (1st Generation)*, AMAZON: AMAZON DEVICES, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E (last visited May 27, 2020). 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* Tony Bradley, *'OK Google' Feature Removed from Chrome Browser*, FORBES (Oct. 17, 2015, 10:48 AM), https://www.forbes.com/sites/tonybradley/2015/10/17/ok-google-feature-removed-from-chrome-browser/#16bc888e76fd; *Google Home*, IDSA (2017), https://www.idsa.org/awards/idea/consumer-technology/google-home; *Top 22 Intelligent Personal Assistants or Automated Personal Assistants*, PAT RES, http://www.predictiveanalyticstoday.com/top-intelligent-personal-assistants-automated-personal-assistants/#content-anchor (last visited May 27, 2020). Google claims that for all the devices with Google Assistant, they would only process speech after the wake word is detected. *See* Sharon Gaudin, *How Google Home's 'Always On' Will Affect Privacy*, COMPUTERWORLD (Oct. 6, 2016, 12:15 PM), http://www.computerworld.com/article/3128791/data-privacy/how-google-homes-always-on-will-affect-privacy.html. Subsequently, Amazon declares that they store voice recordings from users only after they are intentionally triggered. *See* Sapna Maheshwari, *Hey, Alexa, What Can You Hear? and What Will You Do With It?*, N.Y. TIMES (Mar. 31, 2018), https://www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html?action=click&module=Intentional&pgtype=Article.

other IoT devices like the Nest Cam operate in an always-on mode, constantly capturing and transmitting data.[26]

The IoT world is growing rapidly, leading to a potential increase in datamining and surveillance.[27] The architecture of some IoT devices might take this argument a step-further. Those IoT devices that operate in a so-called always-ready or always-on mode are potentially capable of collecting data without activation. These devices take surveillance capabilities a step further as they shift the paradigm of constant collection and retention of data from opt-in to opt-out. Unlike when someone uses the internet and "turns it on," always-on devices are shifting datamining into an active collection of information.

Under this datamining-by-default paradigm, many individuals in modern society are becoming subjected to almost constant surveillance. This potential paradigmatic change naturally affects many members of modern society and could eventually lead society into an always-on era.[28] But the potential negative impact on individuals' civil rights and liberties—and perhaps mostly on their right to privacy—could be direr for some vulnerable populations than others, as technology does not generally differentiate between users. One of these vulnerable populations is that of children, whose data could be just as valuable as that of adults.[29] But even if an IoT device does not purposely mine children's data, it might be inevitable for some of these devices to do so due to their datamining-by-design architecture. To understand the potential negative impact on children's privacy in this context, it is crucial to first scrutinize the interaction of children and IoT.

26. The Nest Cam "begin[s] recording and transmitting audio when turned on, and [is] designed to continue recording and transmitting data 100% of the time or until manually turned off." *See* STACEY GRAY, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES 3–6 (2016).

27. An example of such an expansion could be that of medical devices like pacemakers and insulin pumps that have internet connectivity. *See* Katherine E. Tapp, *Smart Devices Won't Be Smart Until Society Demands an Expectation of Privacy*, 56 U. LOUISVILLE L. REV. 83, 84 (2017). For more on IoT devices, see April Glaser, *Philip K. Dick Warned Us About the Internet of Things in 1969*, SLATE (Feb. 10, 2015, 5:27 PM), http://www.slate.com/blogs/future_tense/2015/02/10/philip_k_dick_s_1969_novel_ubik_on_the_internet_of_things.html; Joseph Steinberg, *These Devices May Be Spying on You (Even In Your Own Home)*, FORBES (Jan. 27, 2014, 9:15 AM), http://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/#15407ce56376.

28. *See* discussion of the 'always-on' era *infra* Part IV.

29. Personal information could be used or sold to third parties for various purposes, including marketing. It could be used for purposes of direct marketing, by which advertisements will be personalized and focused. As evident from the internet, marketers actively pursue children as influential consumers, as they both have their own spending powers and they could also influence their friends and parents. *See, e.g.*, Danielle J. Garber, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 140–45 (2001) (describing the value of information in general, and that of children specifically); Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. Spring 2000, ¶¶ 59–62.

B. Children and the Internet of Things

Children's interaction with technology could be traced back to the invention of mechanical toys around 400 BC—like that of the flying pigeon of Archytas of Tarentum.[30] These toys were further developed through time, mainly since the sixteenth century due to the inventions of Leonardo da Vinci and Galileo Galilei, continuing until the nineteenth century—an era that some had dubbed the "golden age of mechanical toys."[31] Some toys were driven by clock mechanisms, while others were driven by springs or friction.[32] The first-ever talking doll was introduced to the world in 1890 when Thomas 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.[33]

Many years later, the digital era arrived. Starting in the 1950s—and mainly since the 1970s—children began to play video games, using consoles and computers.[34] The advent of mainframe computer games and home consoles in the 1980s further expanded children's interaction with the digital era, as they were now able to play games in video arcades and in their own homes.[35] The digital childhood broadly expanded with the commercialization of the internet. Children were exposed to a new era, that of online gaming. Simultaneously, consoles had been further developed, granting children additional ways to play games within their homes, while sometimes being connected to the internet.[36] An analog childhood began to disappear from the modern world.

The impact of the internet on children's lives could be vast.[37] But beyond the possibilities that the internet entailed, it also introduced a new entity within the child's play or interaction with technology—that of intermediaries. Prior to the internet, children did not generally interact with any intermediary. Once a toy or a device was purchased, it could be used without external intervention or monitoring. With the invention of the internet and upon being granted access, children were suddenly able to interact with various forms of Online Service Providers ("OSPs") from the moment of connecting to the internet for any online activity in which they engaged.[38] These days, children are often exposed to the

30. *See History of Mechanical Toys: How It All Began and Where Are Mechanical Toys Today*, RETRO TOYS, http://re.trotoys.com/article/mechanical-toys-history (last visited May 27, 2020).

31. *Id.*

32. *Id.*

33. *See* Victoria Dawson, *The Epic Failure of Thomas Edison's Talking Doll*, SMITHSONIAN MAGAZINE (June 1, 2015), http://www.smithsonianmag.com/smithsonian-institution/epic-failure-thomas-edisons-talking-doll-180955442; James Vlahos, *Barbie Wants to Get to Know Your Child*, N.Y. TIMES MAG. (Sept. 16, 2015), https://www.nytimes.com/2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html.

34. For a general review of the history of video games, see MARK J. P. WOLF, THE VIDEO GAME EXPLOSION: A HISTORY FROM PONG TO PLAYSTATION AND BEYOND 35–44 (Mark J.P. Wolf ed., 2008).

35. *Id*. at 53–58.

36. For more on online games, see TRISTAN DONOVAN, REPLAY: THE HISTORY OF VIDEO GAMES 265–79 (2010).

37. For more on the impact of the internet on children, see, for example, Martin Valcke et al., *Internet Parenting Styles and the Impact on Internet Use of Primary School Children*, 55 COMPUTERS & EDUCATION 454 (2010).

38. *See infra* note 39.

internet at very early stages of their lives.[39] Whether by using family-shared devices or having access to it on their own, the use of the internet now starts earlier and earlier.[40] To connect to the internet, children simply need access to computers, smartphones, or tablets, to name but a few examples.[41] Some might join the social media world, if they have not already done so, and new apps targeted towards children might further increase their online participation.[42] Essentially, they are the natives of this digital world.[43]

Children's interactions with technology could continue to increase due to IoT. In some instances, the exposure to IoT is a rather passive one.[44] It occurs through parental monitoring conducted in relatively early stages of their lives, from fetuses to young children.[45] Their passive use of IoT might continue through various forms of sensors, monitors, and wearables that their parents—or other caregivers—use to ensure their personal safety, growth, health, and development.[46] But upon reaching some level of skills like communication and independence, IoT could actively become integral in their lives, whether directly or inadvertently. Due mostly to connectivity and mobility, IoT might constantly

39. For a general survey of children's internet use as of 2013, see DONELL HOLLOWAY ET AL., LSE, ZERO TO EIGHT: YOUNG CHILDREN AND THEIR INTERNET USE (2013), http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf.

40. *See* Antigone Davis, *Hard Questions: So Your Kids Are Online, But Will They Be Alright?*, FB: NEWSROOM (Dec. 4, 2017), https://newsroom.fb.com/news/2017/12/hard-questions-kids-online ("Some 93% of 6-12 year olds in the US have access to tablets or smartphones, and 66% have their own device.").

41. For more on children's participation in the online environment, see generally Sonia Livingstone, *Maximising Opportunities and Minimising Risks for Children Online: From Evidence to Policy*, 37 INTERMEDIA 50 (2009).

42. Recently, Facebook released a new chat app targeted towards children aged six to twelve. *See* Ali Breland, *Facebook App for Kids Sparks Privacy Concerns*, HILL (Dec. 12, 2017, 8:30 AM), http://thehill.com/policy/technology/364050-facebook-app-for-kids-sparks-privacy-concerns.

43. *See generally* JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008) (generally discussing "digital natives"—those who grew up in the digital age, as opposed to the digital immigrants). Others have termed those who were born between 1995 and 2012 as "iGen". *See* Jean M. Twene, *Have Smartphones Destroyed a Generation?*, ATLANTIC (Sept. 2017), https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198 (describing iGen as "members of this generation [who] are growing up with smartphones, have an Instagram account before they start high school, and do not remember a time before the internet.").

44. *See infra* note 45 and accompanying text.

45. Monitoring could occur prior to birth by the use of ultrasound screening. *See* Gaia Bernstein & Zvi Triger, *Over-Parenting*, 44 U.C. DAVIS L. REV. 1221, 1232 (2011); Deborah Lupton & Ben Williamson, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, 19 NEW MEDIA & SOC'Y 780, 783–84 (2017). Currently, caregivers could make use of various IoT devices that would aid them in protecting their babies. Examples of such devices include devices with sensors that monitor the baby's respiration rate, temperature, sleep, body position and activity level; smart changing pads and bottle makers (devices that target, *inter alia*, an infant's physical development and bowel movements); baby-movement monitors; smart anti-drowning devices; and smart devices that measure a child's vitals. *See* Abby Adams, *Parenting Life Hacks: Top IoT Products in Baby Care*, IOT EVOLUTION (Mar. 7, 2018), https://www.iotevolutionworld.com/smart-home/articles/437360-parenting-life-hacks-top-iot-products-baby-care.htm.

46. *See generally* Bernstein & Triger, *supra* note 45, at 1232–33; Lupton & Williamson, *supra* note 45; Margaret K. Nelson, *Watching Children: Describing the Use of Baby Monitors on Epinions.com*, 29 J. FAM. ISSUES 516 (2008).

surround them. Depending on the purpose behind the use of IoT, the direct exospore to IoT could be divided into two categories: caregiver-focused and children-targeted.

Caregiver-focused IoT devices are devices or tools that are directly and purposely used by children and generally controlled by their caregivers for the purpose of communication or parental control, for the child's own personal safety or health.[47] Child-tracking devices could serve as an example of caregiver-focused IoT devices.[48] These devices could, for instance, include children's GPS watches and other wearables, designed to grant parents some form of control over their children's activities and locations.[49] Other devices might simply monitor children's behavior, to monitor and detect, *inter alia*, whether they brush their teeth, drink water, behave properly, or inappropriately interact with other individuals or are contacted by them.[50] Caregiver-focused IoT devices could potentially also be used by state agencies as a form of childhood governance—to ensure their safety; promote their health, development, and educational progress; and to ensure that they become productive citizens.[51]

Children-focused IoT devices are devices or tools that are controlled mainly by children, serve purposes that would aid the child (*e.g.*, providing educational, social, or entertainment value), and are used for reasons other than monitoring or safety.[52] Children-focused devices consist of various toys and gadgets. One common example is that of connected smart toys, *i.e.*, toys that are communicative to children via IoT ("IoToys"). Hello Barbie exemplifies such toys—a doll that "actually listens and talks back."[53] This device connects to the internet via Wi-Fi and by the press of a buckle button on its belt turns its microphone on and

47. Notably, this form of control is often used for web browsing, whereas the parent has the ability to record computer activity, block certain web content, or be notified when sensitive content appears on the screen. *See* Alexei Czeskis et al., *Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety*, SOUPS (July 2010), https://cups.cs.cmu.edu/soups/2010/proceedings/a15_czeskis.pdf.

48. *See id*.

49. *See* Rebecca Edwards, *The Best Kids GPS Trackers and Wearables*, SAFEWISE, https://www.safewise.com/resources/wearable-gps-tracking-devices-for-kids-guide (last updated Apr. 22, 2020). For teenagers, parents might use technology that will provide them with real-time location and speed of the driver or even watching them. *See* Alexei Czeskis et al., *supra* note 47, at 2.

50. IoT toothbrushes could, for instance, encourage children to brush properly by using various types of incentives like games. For an example of such a toothbrush, see *This Electric Toothbrush Uses Games to Encourage Kids to Brush Their Teeth*, IRISH EXAMINER (July 30, 2018, 4:52 PM), https://www.irishexaminer.com/breakingnews/technow/this-electric-toothbrush-uses-games-to-encourage-kids-to-brush-their-teeth-858809.html. LeapFrog LeapBand is an example of a wearable device that encourages children to be physically active. *See* Lupton & Williamson, *supra* note 45, at 784. The hydration tracker is a physical water bottle, which upon entering a child's biographical and personal information computes a consumption goal which is logged and can be viewed from within an application. *See* Gordon Chu et al., *Security and Privacy Analyses of Internet of Things Children's Toys*, 6 IEEE 1 (2018).

51. *See* Lupton & Williamson, *supra* note 45, at 783.

52. *See id.* at 781.

53. *See* Katie Lobosco, *Talking Barbie is Too 'Creepy' for Some Parents*, CNN BUSINESS (Mar. 12, 2015, 4:11 PM), http://money.cnn.com/2015/03/11/news/companies/creepy-hello-barbie. Notably, however, Hello Barbie's future lies in great uncertainty due to Apple's acquisition of Pullstring—the company that was in charge of Hello Barbie voice analysis. *See* Brain Raftery, *Apple Acquires Voice-Tech Company Behind 'Hello Barbie'*, FORTUNE (Feb. 15, 2019, 5:44 PM), https://fortune.com/2019/02/15/apple-acquires-pullstring-voice-technology.

begins recording.[54] The data is then sent from the doll to a cloud-based service of ToyTalk and, following an analysis, a response is streamed back to the user through the doll's speaker.[55] Within this market, another example is that of My Friend Cayla, a doll that can interact with users by playing games, sharing photos, and reading them stories.[56] Within the IoToys realm, other examples include the Hello Barbie Dreamhouse, a smart connected home for Barbie dolls;[57] a smart toy bear that "talks, listens, and 'remembers' what your child says and even responds when spoken to";[58] and cloud-connected toy dinosaurs that listen to children's questions and answer according to their age.[59]

But IoToys are merely the beginning when it comes to children's interactions with IoT. Much like adults, children can now use computerized personal assistants, some even directly targeted at them. Amazon, for instance, offers the Echo Dot "Kids Edition"—a standard Echo Dot with "parental controls, kid-friendly content, and an optimized experience for kids."[60] While much uncertainty still lies, Mattel had planned to release a computerized personal assistant named Hello Barbie Hologram—a small box with an animated projection of Barbie that responds to voice commands following the use of a wake phrase.[61] One final example of IoT devices directed at children is that of video game consoles such as Xboxes that are embedded with "Kinect"—an always-on motion-sensing input device.[62]

The potential exposure of children to IoT does not stop at IoToys or devices that are directly targeted towards them. They might be exposed to IoT devices anywhere these devices operate, and perhaps mainly, within their own homes. Depending mostly on their age, skills and abilities, children might use smart refrigerators, smart toasters, smart TVs, or computerized personal assistants like Amazon Echo or Google Home, to name but a few examples. They might even find IoToys limited and boring in comparison to other smart devices and thus

54. *See* Iain Thomson, *Hello Barbie: Hang On, This Wi-Fi Doll Records Your Child's Voice?*, REG. (Feb. 19, 2015, 7:39 AM), http://www.theregister.co.uk/2015/02/19/hello_barbie.

55. *See* Lobosco, *supra* note 53; Joseph Steinberg, *This New Toy Records Your Children's Private Moments—Buyer Beware*, FORBES (Mar. 20, 2015, 2:51 PM), http://www.forbes.com/sites/josephsteinberg/2015/03/20/this-new-toy-records-your-childrens-private-moments-buyer-beware/#2d7698951ab9.

56. Upon downloading the app, users can ask Cayla questions which will be answered by "Internet sources" like Google Search, Wikipedia, and Weather Underground. MY FRIEND CAYLA, https://www.genesis-toys.com/my-friend-cayla (last visited May 27, 2020).

57. *Barbie Hello Dreamhouse*, BARBIE, https://barbie.mattel.com/shop/en-us/ba/dollhouses/barbie-hello-dreamhouse-DPX21 (last visited May 27, 2020).

58. *Smart Toy Bear*, MATTEL FISHER-PRICE, https://m.service.mattel.com/us/Technical/productDetail?prodno=DNV31&siteid=27 (last visited May 27, 2020).

59. *CogniToys: Internet-Connected Smart Toys that Learn and Grow*, KICKSTARTER, https://www.kickstarter.com/projects/cognitoys/cognitoys-internet-connected-smart-toys-that-learn (last visited May 27, 2020).

60. *See* Dan Seifert, *Amazon's New Echo Dot Kids Edition Comes with a Colorful Case and Parental Controls*, VERGE (Apr. 25, 2018, 7:25 AM), https://www.theverge.com/2018/4/25/17276164/amazon-echo-dot-kids-edition-freetime-price-announcement-features-specs.

61. *See* Tim Moynihan, *So, Barbie's a Hologram Now. Oh, and She Responds to Your Voice*, WIRED (Feb. 17, 2017, 9:00 AM), https://www.wired.com/2017/02/hello-barbie-hologram-matell.

62. *See* John Keilman, *Is My Xbox Spying On Me?*, CHI. TRIB. (Jan. 1, 2016, 2:00 AM), http://www.chicagotribune.com/news/ct-toys-online-spying-keilman-hf-0106-20160101-column.html; EPIC Letter to the Attorney General and the FTC Chairwoman, *supra* note 22, at 3.

might prefer using adults' IoT devices.[63] These devices could offer children many things, like asking questions and playing music, but among other features could also be embedded with many "skills" that are directed at them and thus could be used for activities like reading bedtime stories and playing lullabies, among others.[64]

At this point, one might question the magnitude of exposure of children to IoT in general, and whether such exposure differs from the already given exposure that occurs via the use of internet. Undoubtedly, the internet has already subjected children to surveillance and datafication by various intermediaries.[65] It has broadened the surveillance capabilities of entities to spy on children, as online operators and intermediaries were placed in a position that enabled them to collect data on children much like on adults.[66] Without legal intervention—or other forces that would push against these practices—children's online activities would subject them to mass data collection, which could have included, *inter alia*, what they searched, what they messaged, where they were, and generally anything that they were doing online.[67] Moreover, children's exposure to IoT could greatly differ around the world. The level of exposure would depend on various factors like connectivity, costs, and necessity.[68] The exposure to IoT might rely on social, cultural, or other differences, even within the same state, city, or town.

Broadly speaking, however, children in modern societies will likely become more exposed to IoT in the near future.[69] If we are in fact moving towards a society driven, at least partially, by smart objects, then there will be little escape for children from interacting with this hyperconnected world. They will live in a smart home, within a smart city, a smart state, and subsequently—a smart world. Such exposure means that IoT might even take datafication of children up a few steps.[70] Generally speaking, IoT devices do not substitute all internet activities, meaning that they could potentially add to the already mass collection of data online. But what could mainly increase the datafication of children by IoT is its

63. *See* Emily McReynolds et al., *Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys*, FTC (May 11, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/11/00038-141895.pdf.

64. In the context of Amazon Echo, see Emily DeJeu, *6 Ways the Amazon Echo Will Transform Your Child's Bedtime Routine*, BABY SLEEP SITE, https://www.babysleepsite.com/sleep-training/amazon-echo-bedtime-routine (last updated Jan. 31, 2020).

65. *See* Lupton & Williamson, *supra* note 45, at 782.

66. *See id.* at 783.

67. *See id.* at 785.

68. It would be inaccurate to assume that all children are affected equally by technology. Simply to exemplify, in some parts of the world, children do not use digital technology at all, and are therefore, obviously, less affected by the use of technology. *See* Roberto A. Ferdman, *4.4 Billion People Around the World Still Don't Have Internet. Here's Where They Live*, WASH. POST (Oct. 2, 2014, 7:30 AM), https://www.washingtonpost.com/news/wonk/wp/2014/10/02/4-4-billion-people-around-the-world-still-dont-have-internet-heres-where-they-live/?utm_term=.4c89f1fcd8cf.

69. It is estimated that the global IoT market will grow from $157B in 2016 to $457B by 2020. *See* Louis Columbus, *2017 Roundup of Internet of Things Forecasts*, FORBES (Dec. 10, 2017, 8:47 PM), https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#6cf48aa41480.

70. *See* Gaudin, *supra* note 25.

architecture. IoT could be equipped with many sensors that could capture the voices, conversations, locations, and even imagery of anyone within the vicinity of the device.[71] As some devices operate in an always-on mode, unlike the internet, IoT could be collecting data even without active use by its user, perhaps even without the user's awareness.[72]

The architecture of IoT devices also increases the possible types of communication, making IoT more accessible, at least to some children. Young children, for instance, could rather easily operate voice activated IoT devices like the Amazon Echo, thus being datafied prior to knowing how to use a computer, and even without knowing how to read or write. Architecture could also affect how devices appeal to children, and the potential variety of devices could further increase such appeal and, subsequently, children's datafication.[73] Some IoT devices are generally also more portable than the traditional computer, meaning that children could take IoT devices with them, making them subjected to datafication for longer periods.[74] These devices could also be considered as less secure than websites in the sense that interested parties might also hack them more easily and gain access to their data.[75] Finally, unlike the internet, IoT might be embedded within a child's surroundings, even as a necessity, thus the child might be required to use IoT throughout his or her daily routine, when performing actions such as opening the door, the refrigerator, or using the microwave.

All in all, IoT increases the potential surveillance and datafication of individuals in modern society, and that includes children. Along with its potential benefits, it also subjects them to potential risks. The use of IoT could, for instance, expose them to harmful content,[76] or have negative psychological effects.[77] Hacking IoT devices or the data they store might lead to inappropriate contact,

71. *See*, *e.g.*, EPIC Letter to the Attorney General and the FTC Chairwoman, *supra* note 22.

72. *See id.* at 5.

73. If, for instance, the IoT device is using animated characters or child-oriented activities and incentives, this practice might increase the probability that a child will want to make use of the device. One example is that of the use of Mickey Mouse as a design for Google's computerized personal assistant (Google Home). *See OtterBox Den Series featuring Disney® Mickey Mouse*, GOOGLE STORE, https://store.google.com/us/product/otterbox_disney_home_base_for_home_mini (last visited May 27, 2020).

74. *Compare LeapStart 3D Learning System*, LEAPFROG, https://store.leapfrog.com/en-us/store/p/leapstart-3d/_/A-prod80-603900 (last visited May 27, 2020), *with Desktop Computers & All-in-Ones*, DELL, https://www.dell.com/en-us/shop/dell-desktop-computers/sc/desktops (last visited May 27, 2020).

75. Serious security flaws were discovered in smartwatches for children, whereby unauthorized individuals could easily seize control of the watches and use them to track and eavesdrop on children. Øyvind H. Kaldestad *Significant Security Flaws in Smartwatches for Children*, FORBRUKERRÅDET (Oct. 18, 2017), https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children. For more on the insecurity of IoT, see BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPERCONNECTED WORLD 19–44, 56–78 (2018).

76. Exposure to harmful content could occur, for instance, when a child is capable of asking Amazon Echo anything she desires, and therefore is vulnerable to listening to harmful results. It could occur deliberately, if the child desires access to the content, or even accidently, when a child asks for something which suits her age, but due to an error of understanding her request, the device produces inappropriate results which could be harmful. *See* Alyssa Pereira, *Amazon's Alexa Mishears Child, Tries to Serve Him Porn*, (SFGATE Dec. 30, 2016, 12:34 PM), https://www.sfgate.com/tech/article/Amazon-Alexa-mishears-child-tries-to-serve-him-10827054.php (showing how a child asked Alexa to "Play Digger," which in turn spouted porn-related results).

77. See Twene, *supra* note 43, for more on the mental-health issues linked to the internet.

sexual exploitation, identity theft, and perhaps even abduction, to name but a few risks.[78] Without belittling such risks, one of the biggest threats in the context of this Article is that of children's privacy: children's personal information could be obtained through their use of IoT devices, with or without their or their parents' knowledge or consent, and thus could be used and misused by third parties.[79] Such potential use or misuse of children's data raises a rather old fear: how to protect children's privacy from a society that is driven towards a ubiquitous surveillance era. Thus, beyond concerns for personal safety, datamining and online surveillance of children raise the need to protect their fundamental rights and liberties, and as the next part scrutinizes, mainly their right to privacy.

III. PRIVACY WITHIN THE INTERNET OF CHILDREN

During childhood, one is considered entitled to special care and assistance.[80] Broadly speaking, such special care and assistance are important as children might lack sufficient skills and cognitive abilities to comprehend risks and concerns as adults do. They might be more trusting than adults are and lack the requisite maturity, ability, knowledge, and experience to protect themselves properly.[81] As a cohort, they are often treated as those in need of protection, as they might be vulnerable to various risks and harms.[82] Not surprisingly, parents are often concerned about their children's interaction with strangers or people they do not know, both offline and online.[83] In fact, children today are watched over more than any other generation in history.[84]

Much like many prior technologies, the internet broadened the potential risks to children, including potential surveillance and datamining.[85] Aside from

78. *See* COMM. ON COMMERCE, SCI., AND TRANSP., CHILDREN'S CONNECTED TOYS: DATA SECURITY AND PRIVACY CONCERNS 4 (2016), https://www.hsdl.org/?abstract&did=797394 [hereinafter Children's Connected Toys]. See SUBCOMM. ON SOC. SEC., FED. TRADE COMM'N, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION BEFORE HOUSE COMMITTEE ON WAYS AND MEANS (2011), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-child-identity-theft/110901identitythefttestimony.pdf, for further information on identity theft of children; *see also More Than 140,000 Children Could Be Victims of Identity Fraud Each Year*, ID: ANALYTICS (July 12, 2011), http://www.idanalytics.com/blog/press-releases/140000-children-victims-identity-fraud-year.

79. *More Than 140,000 Children Could Be Victims of Identity Fraud Each Year*, *supra* note 78.

80. *See* JOHN PALFREY ET AL., BERKMAN CTR. FOR INTERNET & SOC'Y, ENHANCING CHILD SAFETY AND ONLINE TECHNOLOGIES: FINAL REPORT FOR THE INTERNET SAFETY TECHNICAL TASK FORCE (2008), https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf, for more on online risks to children.

81. *See* Garber, *supra* note 29, at 132; 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).

82. Hertzel, *supra* note 81, at 434.

83. *See* Davis, *supra* note 40 ("74% of parents of 6-12 year olds are concerned about their children interacting with strangers or people they don't know online . . . .").

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

85. The potential risks of technology to young children emerged prior to the internet. In the 1970s, following the advocacy of child-advocacy and consumer groups, The Federal Communications Commission ("FCC") sought to regulate the potential exposure to advertising by setting policy guidelines for TV commercials targeted at children under the age of twelve. This regulatory attempt met a backlash from both the industry and the media, and resulted in the FCC taking a step back from what was termed as the "kidvid controversy". *See, e.g.*, Dale

various risks that the internet entails, the potential surveillance and datafication of children might pose a vivid threat to their privacy. To address the threats that arose from the internet, many policy-makers, including those in the U.S., introduced a regulatory framework to protect them.[86] To gain a better understanding of the privacy risks that IoT poses to children, this part will be further divided into two subparts. The first subpart explores the legal protection of children's privacy under the current legal framework. The following subpart will then show that while this regulatory framework currently governs children's usage of IoT to some extent, it fails to properly protect children's privacy from the datafication by many IoT devices.

A. Children's Right to Privacy

The right to privacy in the modern era is famously attributed to a Harvard Law Review Article, written by Samuel Warren & Louis Brandeis.[87] Since then, many scholars attempted to conceptualize privacy in various ways.[88] On a practical level, the protection of privacy is granted generally through various legal mechanisms, like the Constitution, federal and state legislation, and other forms of regulation.[89] Categorially, the American approach towards information privacy is considered sectoral in nature,[90] *i.e.*, federal law that is directed towards

Kunkel, *Policy Battles About Defining Children's Educational Programming*, 557 ANNALS OF THE AM. ACAD. OF POL. AND SOC. SCI. 39–53 (1998); 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).

86. Notably, the importance of protecting children from harm was formally acknowledged at the international level in 1989 with the United Nations' adoption of the Convention on the Rights of the Child. This convention, ratified by all UN member states (with some reservations or interpretations) except the U.S., generally protects children under the age of eighteen on various grounds, *e.g.*, the protection of children's right to life, survival and development; to have their best interests respected; to nondiscrimination; to be heard; the right to identity; information and media of their choice; education; protection from violence and sexual exploitation; and freedom of expression, thought and association. *See* United Nations Convention on the Rights of the Child art. 2, 3, 8, 12–17, 19, 28–30, Nov. 20, 1989, 28 I.L.M. 1448, *corrected* at 29 I.L.M. 1340 (1990). Among these rights, the UN acknowledged the need to protect privacy. *See id*. at art. 16 ("No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation . . . The child has the right to the protection of the law against such interference or attacks.").

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

88. For instance, Alan Westin conceptualized privacy as the right to control information of oneself under the 'control theory'; Ruth Gavison posited that privacy is related to our concern over our accessibility to others under the 'limited access theory'; and Helen Nissenbaum offered a conceptual framework of privacy as contextual integrity which links the protection of personal information to the norms of specific contexts. *See* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMAN IN A FREE SOCIETY 5 (1988); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3 (2010); ALAN WESTIN, PRIVACY AND FREEDOM 5 (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."); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980).

89. *See* Eldar Haber, *Toying with Privacy: Regulating the Internet of Toys*, 80 OHIO ST. L.J. 399 (2019). For a taxonomy of privacy, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 478 (2006).

90. A sectoral approach is contrary to an omnibus approach that regulates privacy consistently across all industries and contexts. *See* Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law, for more on these differences.

specific industries or sensitive contexts or populations.[91] One of these cohorts are children under the age of thirteen, protected to some extent when using the internet.

The protection of children's privacy online was first formally acknowledged with the enactment of COPPA in 1998.[92] COPPA is supplemented by a rule created and updated by the FTC.[93] Enforced by the FTC,[94] COPPA is primarily designed to prohibit unfair or deceptive acts or practices in connection with personal information from and about children on the internet.[95]

As COPPA was drafted to address the privacy risks that stem from the internet, it applies to OSPs that target children under the age of thirteen or knowingly collect personal information from them.[96] Falling under COPPA requires websites to adhere to Fair Information Practice Principles ("FIPPs"),[97] which include notice, consent (choice), access, data minimization, security, and enforcement.[98] More specifically, websites that fall under COPPA must include a *notice*

91. *See generally* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003).

92. 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, is rather limited as it applies only on the release of educational records to unauthorized persons by educational institutions. *See* Family Educational Rights and Privacy Act (FERPA), Pub. L. No. 93-380, 88 Stat. 57 (1974) (codified at 20 U.S.C. § 1232(g) (2018)); *Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T EDU., http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (last visited May 27, 2020); *see also* Montgomery & Chester, *supra* note 85, at 279.

93. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2018)). COPPA Rule is effective since April 2000. See Children's Online Privacy Protection Rule 78 Fed. Reg. 3972 (Jan. 17, 2013), for the latest update.

94. *See* 15 U.S.C. §§ 6501–6506 (2018); 16 C.F.R. § 312.9 (2019). The FTC authority stems from both the Federal Trade Commission Act ("FTC Act"), Ch. 311, §5, 38 Stat. 717 (codified at 15 U.S.C. §§ 45(a), 6505(a) (2018)) and COPPA. It has the authority to promulgate and update rules under the Administrative Procedures Act (codified at 15 U.S.C. § 6502(b) (2018)). *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); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014). Consequently, it can issue fines and seek preliminary or permanent injunctive remedies for those who do not comply with COPPA regulation. *See* 15 U.S.C. §§ 45(l)–(m), 53(b) (2018).

95. 15 U.S.C. §§ 6501–6505 (2018); Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2019)); Garber, *supra* note 29, 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 to both financial harms and unwarranted health and safety risks. *See* Solove & Hartzog, *supra* note 94, at 599; FTC v. Accusearch, Inc., 570 F.3d 1187, 1205 n.4 (10th Cir. 2009) ("[T]he '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 (2018) (unfair methods of competition unlawful).

96. *See* 15 U.S.C. §§ 6501(1), 6501(8), 6502 (2018); 16 C.F.R. § 312.2 (2019).

97. FIPPs could also include accuracy and accountability. *See* Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the Security of Things*, 2017 U. ILL. L. REV. 415, 441 (2017).

98. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS i, 3–4 (May 2000) 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 29, at 153.

containing what information is collected, how collected information is used, and the website's information disclosure practices;[99] obtain *verifiable parental consent* for the collection, use, or disclosure of such personal information;[100] grant parents the ability *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;[101] provide reasonable means, in the given circumstances, for the parent *to obtain any personal information collected from that child*;[102] adhere to *data retention and deletion requirements*;[103] are prohibited from 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;[104] and *establish and maintain reasonable procedures* to protect the confidentiality, security, and integrity of personal information collected from children.[105]

COPPA was essentially crafted to ensure that intermediaries or other third parties do not misuse the data obtained from children under the age of thirteen while they surf the web.[106] In other words, as the internet posed threats to children's privacy, Congress reacted by creating a new regulatory framework, sectoral in nature, that would supposedly increase protection for children's privacy when they enter the online environment.[107] It effectively placed barriers to the datafication of children online in some instances, thus promoting their right to information privacy to some extent.

But the meaning of "being online" or "surfing the web" is constantly on the move, and while the regulatory mechanisms that were set to protect children online might currently be obsolete to deal with technological innovations, the privacy risks of IoT to children might also be different than what Congress sought to initially protect against. Children's privacy interests, however, have not changed and should be protected despite these technological changes. As the next subpart argues, while COPPA regulation currently applies to some IoT devices, it is currently ill-crafted to protect children's privacy properly in IoT, as children's datafication could drastically change due to the use of IoT devices.

B. COPPA and IoT

Whether COPPA applies to IoT operators is dependent on two phases of evaluations: (1) determining whether IoT operators are considered OSPs and (2) determining whether the device targets children under the age of thirteen or

99. 15 U.S.C. § 6502(b)(1)(A)(i) (2018); 16 C.F.R. § 312.4 (2019).
100. 15 U.S.C. § 6502(b)(1)(A)(ii) (2018); 16 C.F.R. § 312.5 (2019).
101. 15 U.S.C. § 6502(b)(1)(B) (2018); 16 C.F.R. § 312.6 (2019).
102. 15 U.S.C. § 6502(b)(1)(B) (2018); 16 C.F.R. § 312.6 (2019).
103. 16 C.F.R. § 312.10 (2019).
104. 15 U.S.C. §§ 6502(b)(1)(C)–(D) (2018); 16 C.F.R. § 312.7 (2019).
105. 16 C.F.R. §§ 312.3(e), 312.6, 312.8 (2019).
106. *See* Garber, *supra* note 29, at 159 n.127.
107. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 902 (2009).

knowingly collects personal information from them.[108] The first evaluation phase is rather simple in this instance. As COPPA only applies to operators of websites or online services, the preliminary requirement in IoT would be to determine whether an IoT operator is considered an OSP under COPPA requirements.[109] COPPA defines an OSP as 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.[110] 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."[111] While there could be various interpretations of the OSP requirement, as, for instance, IoT is not a website *per se*, the FTC has clarified that IoT devices will be deemed a website or online service for the purpose of COPPA regulation.[112] Unless the FTC changes its current interpretation, this requirement is currently met.

The second evaluation phase is less evident. Upon deciding that an IoT operator is considered an OSP under COPPA requirements, one must examine whether the IoT device targets children under the age of thirteen or knowingly collects personal information from them.[113] To simplify, COPPA regulates "websites"—IoT devices in the context of this Article—whereas the OSP collects personal information from children under thirteen years of age when either the service is *directed* towards them or when the OSP *knowingly collects information* from them, even lacking direct targeting.[114]

Here is where the evaluation might get tricky. IoT relates to a broad world of devices and services. Some of them target children under the age of thirteen, but it is highly debatable if others also do so. IoToys devices could serve as a clear example of the first category. Toys are generally designed for young children and, when equipped with internet connectivity, COPPA should and does apply.[115] The same would apply for any IoT devices that are designed or directly advertised as "for children", such as the Echo Dot Kids Edition.[116] These devices

108. *See* 15 U.S.C. §§ 6501(1), 6501(8), 6502 (2018); 16 C.F.R. § 312.2 (2019).

109. Notably, nonprofits or government agencies or institutions will not fall under COPPA regulation, as they are generally exempt from coverage under the Federal Trade Commission Act. *See* 15 U.S.C. §§ 44–45 (2018); 16 C.F.R. § 312.2 (2019). Nonprofit entities, however, that operate websites or services for the profit of their commercial members may be subject to liability under COPPA. *See* 15 U.S.C. § 45 (2018); FTC v. Cal. Dental Ass'n, 526 U.S. 756 (1999).

110. *See* 15 U.S.C. § 6501(2) (2018).

111. *Id.*

112. *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; *see also* Letter from Maureen K Ohlhausen, Acting Chairwoman of the Federal Trade Commission, to Senator Mark R. Warner (June 22, 2017), https://www.scribd.com/document/352278126/2017-06-21-Response-to-Senator-Warner-Letter ("The COPPA Rule applies not only to websites, but also to other online services, including connected toys and associated mobile apps.").

113. *See* 15 U.S.C. §§ 6501(1), 6501(8) , 6502 (2018); 16 C.F.R. § 312.2 (2019).

114. 16 C.F.R. § 312.2 (2019).

115. For more on IoToys and COPPA, see generally Haber, *supra* note 89.

116. *See* Seifert, *supra* note 60.

clearly fall under COPPA, as they are directed towards children and their operators have actual knowledge that they are collecting personal information directly from children.[117]

On the other side of the spectrum are IoT devices that one could categorize as clearly falling outside of COPPA's scope. These would include, for instance, IoT devices that are clearly not directed towards children nor knowingly collect personal information from them. These could include IoT devices designed to be used by adults, like smart cars, smart sex toys, or smart health devices for aiding adult diseases.[118] If the IoT device sets limitations and restrictions for its use, making it accessible only for those that are clearly over the age of thirteen, then we can generally label such a device as outside of COPPA's scope. With potential exceptions, expansive devices that require an account, high costs, and technical abilities to set up might fall under this category in general.[119] For these devices, the OSP will not knowingly collect personal information from children.[120]

The grey area for other devices might be rather large. It becomes more difficult to decide whether COPPA applies when dealing with IoT devices that are not targeting children under the age of thirteen *per se*—or at least not targeting only children—but at the same time could very well be used by them or collect data from them. One clear example would be IoT devices that operate within the home.[121] When many IoT devices are present in homes, they could potentially be used directly by children. Unless such a device prevents use by children under the age of thirteen in some way—for example, by utilizing passwords, biometric activation, or simply a physical inability to activate the device—then children might make use of it. Even if young children do not directly use these devices, their actions could be constantly recorded inadvertently by many of them.

From a legal perspective, it is unclear whether COPPA regulation will deem children as the target audience for these types of devices. Take computerized personal assistants as an example of such unclarity. What is the target audience of computerized personal assistants? One could argue that computerized personal assistants, like Amazon Echo, target adults, as they often require the opening of an account, they can be relatively costly, and their functionality is designed

117. *See* 16 C.F.R. § 312.2 (2019) ("A Web site or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children.").

118. It is generally debatable whether a device targets adults or not, but there are some examples which should not generally raise controversies over their main, and perhaps sole, target audience. For one example, see Malek Murison, *Health IoT: Wearable Can Predict Older Adults' Risk of Falling*, INTERNET OF BUS. (July 13, 2018), https://internetofbusiness.com/health-iot-wearable-predict-risk-falling.

119. Amazon Echo could be a good example for such requirements. *See Set Up Your Echo*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201601770 (last visited May 27, 2020).

120. *See* 15 U.S.C. §§ 6501(1), 6501(8), 6502 (2018); 16 C.F.R. § 312.2 (2019).

121. *See* sources cited *supra* note 120; Haber, s*upra* note 89 at 453–54.

for adults.[122] On the other hand, many of these devices are advertised and sold to families with young children, who might actively or inadvertently use them.[123]

The legal framework attempts to aid in clarifying these grey zones. Under COPPA, determining if an IoT device is directed towards children under the age of thirteen requires the assessment of various factors: (1) subject matter, (2) visual content, (3) use of animated characters or child-oriented activities and incentives, (4) music or other audio content, (5) age of models, (6) presence of child celebrities or celebrities who appeal to children, (7) language or other characteristics of the website or online service, and (8) whether advertising promoting or appearing on the website or online service is directed to children.[124] One potential safe haven for an OSP that argues that it does not target children as its primary audience would be embedding the service with features that restrict children from accessing it, or at least make it highly difficult for children to do so.[125] An example would be when collection of personal information occurs after age verification and when it prevents the collection, use, or disclosure of personal information from visitors who identify themselves as children.[126] Nevertheless, it is practically difficult to make all devices accessible only to adults, and thereby, datafication of children under thirteen will likely occur in many instances.

Assessing these factors could naturally differ between IoT devices. To demonstrate, consider that many IoT companies advertise their products to children and parents with children.[127] In their commercials, they will often use actors portraying how the entire family, adults and children alike, can make use of the IoT device.[128] It might even become more complex due to external add-ons offered by various intermediaries, which might be out of the OSPs' control, but nevertheless raise similar concerns regarding the attraction of the device to children. Think of a Mickey Mouse "outfit" for an Amazon Echo as an example.[129]

122. Amazon Echo, for instance, requires an Amazon account, which is only allowed for 18-year-olds and above. *See Amazon Privacy Notice*, AMAZON (last updated Jan. 1, 2020), https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010&pop-up=1 ("Amazon does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon Services only with the involvement of a parent or guardian. We do not knowingly collect personal information from children under the age of 13 without the consent of the child's parent or guardian").

123. *See infra* note 128.

124. *See* 16 C.F.R. § 312.2 (2019).

125. More specifically, the IoT device will not be deemed directed to children when the OSP does not collect personal information from any visitor prior to collecting age information; and prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under the age of thirteen without first complying with the notice and parental consent requirements as set under COPPA. *See id*.

126. *Id*.

127. *See* Mark Harris, *Virtual Assistants Such as Amazon's Echo Break US Child Privacy Law, Experts Say*, GUARDIAN (May 26, 2016, 7:00 AM), https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law.

128. See, for instance, the first commercial by Amazon for its Echo device, whereas the entire family communicates with the device. *Introducing Amazon Echo*, YOUTUBE (Aug. 5, 2016), https://www.youtube.com/watch?v=CYtb8RRj5r4. Moreover, the (presumably) daughter asks her (presumably) father whether the Echo is "for me," whereby he replies, "it's for everyone." *Id.*

129. See, for instance, the "OtterBox Den Series featuring Disney® Mickey Mouse" for Google Home devices—a "playful Disney Mickey Mouse design" which "[b]ring[s] home the fun and enchantment of Disney." *OtterBox Den Series Featuring Disney® Mickey Mouse*, *supra* note 73.

While the device might not be considered as targeting children under the age of thirteen under COPPA, perhaps it should.

For now, however, suppose that upon assessment, the IoT device is labeled as not targeting children under the age of thirteen. As mentioned, COPPA would still apply if the OSP knowingly collects personal information from them.[130] This requirement could become highly relevant for devices that children could physically use and that might appeal to them. Now, consider IoT devices that are constantly present in a household, like a smart refrigerator, toaster, TVs, and personal assistants like Amazon Echo or Google Home. Depending on the age, development stage, and skills of children, it is safe to argue that at least some of them will use these IoT devices to a certain extent.

In both instances, *i.e.*, regardless of whether the device is directed towards children under the age of thirteen or not, COPPA only applies when the OSP is actually collecting personal information from them. Perhaps not all IoT devices will collect data during the use of the device or will only store the data locally, but generally speaking, data collection is usually an integral part of their operation, and thus the collection of information element will most likely be fulfilled. This information, however, will not necessarily be considered as personal. Personal information is defined under COPPA as "individually identifiable information about an individual collected online."[131] This category could include various types of information, like the full name of a child, her home or physical address, and telephone number, to name but a few examples.[132] For some devices, like Amazon Echo and Google Home, this would be rather evident, as audio recordings containing the voice of a child under the age of thirteen are also considered personal information under COPPA.[133]

The problem, however, is that there is little evidence on what data IoT devices collect *de facto* from their users, let alone from children. While companies must divulge these practices in their privacy policies, it is difficult to evaluate what data is essentially stored and transmitted by at least some IoT devices.[134] Obviously, without clear statements on the collection of information, other devices might require *ex-post* examination to decide whether personal information

130. *See* 15 U.S.C. §§ 6501(1), 6501(8), 6502 (2018); 16 C.F.R. § 312.2 (2019).

131. 15 U.S.C. § 6501(8) (2018).

132. The examples listed under COPPA include: (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 websites 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. 16 C.F.R. § 312.2 (2019).

133. *See id*. Notably, in its original form from 1999, the COPPA Rule defined personal information as including photographs only when combined with additional information that would allow physical or online contacting of the child. The FTC amended the rule in 2013, adding several new types of data to the definition of personal information such as a photograph, video, or audio file that contains a child's image or voice. *See* Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings, 82 Fed. Reg. 58076 (Dec. 8, 2017).

134. *Id.*

was collected. This examination could essentially act as a double-edged sword: lacking analysis of the shared data, OSPs will not be able to determine whether personal information was collected or whether it is that of a child under the age of thirteen or not. It will require OSPs to conduct data analysis that might pose a risk to the privacy interests of those over the age of thirteen. Essentially, such a decision might rely on a cost-benefit analysis of OSPs—they might evaluate the costs and the benefits that are associated with the use of data, costs of implementation (of, say, analytic tools), and the costs of complying with COPPA, to name but a few examples.

Overall, IoT devices that target children under the age of thirteen and collect personal information from them will fall under COPPA regulation. The question now is whether IoT devices that do not target children under the age of thirteen but still collect personal information from them have actual knowledge of such collection, as otherwise it will not fall under COPPA. This assessment might be rather tricky. IoT companies will have knowledge about the collection of personal information, but not necessarily that it is that of a child under the age of thirteen. To a great extent, many companies might adhere to an "ignorance is bliss" approach, by which they are supposedly incapable of knowing whether a given recording is that of an individual under or over the age of thirteen. Some OSPs, like Facebook, have chosen such a path and would be excluded from COPPA as a default, simply by only allowing the opening of an account if the user is over thirteen years of age,[135] and deleting accounts for those proven under that age.[136] Factually, many children bypass these mechanisms and use social media regardless.[137] But COPPA will still not apply to Facebook and its likes, as long as the companies' policy does not allow children under the age of thirteen to partake in their services and unless they have actual knowledge that children under that age use the service.[138]

Furthermore, much like Amazon's move with the Echo Kids edition and Facebook's Messenger Kids—a chat app for those under thirteen—IoT OSPs might attempt to draw a clear line of which service or device should fall under

135. *See* Audrey Watters, *Mark Zuckerberg Wants Kids Under 13 to Join Facebook, Uses Bogus Excuse to Explain Why They Can't*, HACKEDUCATION (May 20, 2011), http://hackeducation.com/2011/05/20/mark-zuckerberg-wants-kids-under-13-to-join-facebook-uses-bogus-coppa-excuse-to-justify-why-they-cant.

136. *See Banning Baby-Faces from Social Site Facebook*, DAILY TELEGRAPH (Mar. 21, 2011, 9:16 PM), https://www.dailytelegraph.com.au/banning-baby-faces-from-social-site-facebook/news-story/c9d888591953e7726dcbfab343e21eb5.

137. *See* Rachel Metz, *Facebook's App for Kids Should Freak Parents Out*, MIT TECH. REV. (Feb. 7, 2018), https://www.technologyreview.com/s/609723/facebooks-app-for-kids-should-freak-parents-out ("Three out of five American parents in a 2017 poll conducted on behalf of Facebook and the National PTA (one of the groups Facebook consulted while building Messenger Kids) said that their under-13-year-olds use messaging apps, social media, or both.").

138. Yelp, for instance, was fined by the FTC in 2014 for knowingly collecting information from children under the age of thirteen as registration through their app required providing users' date of birth. *See* Press Release, FTC, *Yelp, TinyCo Settle FTC Charges Their Apps Improperly Collected Children's Personal Information*, (Sept. 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/09/yelp-tinyco-settle-ftc-charges-their-apps-improperly-collected.

COPPA regulation and which should not.[139] Even more, when third parties wish to design a "for-children" app or skill for an IoT device, they will have to adhere to COPPA by design.[140]

The problem, however, is that this so-called "solution" is not pragmatic to safeguard children's privacy. For one, children could easily bypass such a mechanism by simply supplying false information. But perhaps more importantly, such a move disregards the personal information that is effectively collected by the device that does not fall under COPPA. Many IoT OSPs will effectively collect personal information on children, and COPPA will not apply, due to the vagueness of its "all-or-nothing" approach, *i.e.*, that if the IoT device does not fall under COPPA, regulation will not apply to protect some children under the age of thirteen; while their personal information might very well be processed by commercial entities.

At its core, COPPA must be revisited and recalibrated to meet the challenges that IoT raises and its differences from the internet that is regulated under COPPA.[141] The regulatory framework that governs those devices that clearly fall under COPPA, like IoToys devices, must be recalibrated within the notion that online websites are not necessarily akin to IoT devices and that proper modifications are required. COPPA, for example, must promote awareness of caregivers to the risks of datafication, increase oversight and accountability on obtaining verifiable consent for the use of these devices, and adhere to stricter data minimization,[142] and transparency requirements.[143] It must also be stricter and clearer regarding the handling of children's data and its security, unlike the current vagueness of establishing and maintaining "reasonable procedures" to protect the data;[144] and the FTC must strongly enforce any deviation from COPPA's rules.[145] IoToys and any children-targeted devices must adhere to a higher

139. *See* Metz, *supra* note 137. Facebook, for instance, guaranteed that the app will not contain advertisements nor sell children's data it collects to third-party advertisers. *See* Breland, *supra* note 42; *Messenger Kids Privacy Policy*, FACEBOOK HELP CENTER, https://www.facebook.com/legal/messengerkids/privacypolicy (last visited May 27, 2020).

140. See, for instance, the "Alexa Skills Kit" for children-targeted skills (known as "Kid skills"). *Create Kid Skills for Alexa*, AMAZON ALEXA, https://developer.amazon.com/alexa-skills-kit/kids (last visited May 27, 2020).

141. Much like the FTC had previously amended the COPPA Rule "to keep pace with changes to technology, children's increased use of mobile devices, and the development of new business models that did not exist when the Commission issued the Rule in 1999." Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings, 82 Fed. Reg. 58076 (Dec. 8, 2017) (to be codified at 16 C.F.R. pt. 312). Notably, Congress is currently considering recalibration of COPPA. *See* Matt Laslo, *Senators on Protecting Kids' Privacy: 'It's Complicated'*, WIRED (Aug. 30, 2019, 4:56 PM), https://www.wired.com/story/senators-protecting-kids-privacy-complicated.

142. Data minimization refers generally to a practice of limiting collection of personal information to that which is directly relevant and necessary for the operation of the service. Bernard Marr, *Why Data Minimization is an Important Concept in the Age of Big Data*, FORBES (Mar. 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#718912f1da45.

143. For these and other proposals, see Haber, *supra* note 89, at 436–37.

144. *See* 16 C.F.R. §§ 312.3(e), 312.6, 312.8 (2018).

145. *See, e.g.*, Tony Romm & Elizabeth Dwoskin, *FTC Approves Settlement with Google over YouTube Kids Privacy Violations*, WASH. POST (July 19, 2019), https://www.washingtonpost.com/technology/2019/07/19/ftc-approves-settlement-with-google-over-youtube-kids-privacy-violations.

threshold, as many of these devices—sometimes COPPA-compliant—were found to have serious vulnerabilities.[146] Thus, COPPA must increase overall security and enforcement of these devices and the stored data obtained through them.[147]

But as this Article further argues, recalibrating COPPA to only meet the challenges of IoToys devices and their likes will merely govern a fraction of IoT devices, and children's datafication might very well continue through those devices that fall under the radar. In other words, while COPPA might apply to some IoT devices, like IoToys, it will fail to apply to many other IoT devices that will effectively be used by children under the age of thirteen. It thus fails to properly protect children against their datafication by various entities. It means that most IoT companies who potentially collect data from children under the age of thirteen and make use of such data are not required to adhere to safeguards that are granted by COPPA, and children are therefore left without legal safeguards for their information privacy. Aside from what is conveyed under privacy policies, terms-of-service ("ToS") agreements, or end-user license agreements ("EULAs"), caregivers will not be notified of the datafication of their children nor grant their consent for such datafication; and will generally lack the ability to obtain a description of datafication or the ability to obtain the data. Additionally, the OSP will not be required to adhere to data retention and deletion requirements nor to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

To a considerable extent, the smartification of the modern world might suggest that recalibrating COPPA is no longer sufficient to protect children from online privacy risks. The transition from the internet to IoT is not merely categorial in nature, but rather substantive, and thus other approaches to children's privacy should be considered by policy-makers, as COPPA might be proven as an

146. Researchers found vulnerabilities in many of these devices, ranging from IoToys like Hello Barbie, and perhaps especially My Friend Cayla, to hydration trackers. *See* Chu et al., *supra* note 50, at 1; Richard Chirgwin, *Hello Barbie Controversy Re-ignited with Insecurity Claims*, REG. (Nov. 29, 2015, 10:58 PM), http://www.theregister.co.uk/2015/11/29/hello_barbie_controversy_reignited_with_insecurity_claims; Darren Orf, *Hackers Found a Way to Make Furbies Even Creepier*, GIZMODO (Feb. 9, 2016, 10:42 AM), http://gizmodo.com/hackers-found-a-way-to-make-furbies-even-creepier-1756683110 (hacking Furby); Lorenzo Franceschi-Bicchierai, *One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*, VICE: MOTHERBOARD (Nov. 27, 2015, 10:08 AM), 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); Samuel Gibbs, *Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children*, GUARDIAN (Nov. 26, 2015, 6:16 AM), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children (hijacking a Hello Barbie); Alex Hern, *CloudPets Stuffed Toys Leak Details of Half a Million Users*, GUARDIAN (Feb. 28, 2017, 9:59 AM), 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); Mark Stanislav, *R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy® hereO GPS Platform Vulnerabilities (FIXED)*, RAPID7 (Feb. 2, 2016), https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform; Danny Yadron, *Fisher-Price Smart Bear Allowed Hacking of Children's Biographical Data*, GUARDIAN (Feb. 2, 2016, 9:00 AM), 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 flaws that would allow hackers to obtain data).

147. *See* Haber, *supra* note 89, at 453.

obsolete model of regulation in this era. Such an approach must take into account that modern society might very well be on the verge of being monitored at almost any given time. As members of society, children are also part of this ubiquitous surveillance era,[148] and much like adults, they might make use of IoT devices as long as these are accessible to them. Their potential exposure greatly increases when—in addition to everyday IoT devices—some "things," like toys that are based on IoT, are directed towards them.

As this Part argued, the question of whether COPPA applies to IoT devices or not might be tricky. Nonetheless, one major concern regarding the protection of children is that IoT-based devices do not generally distinguish between the use of adults or children, making it almost impossible for general-use IoT devices to fall under any regulation that is designed to protect only a specific cohort, such as children. Thus, as the next Part shows, protecting children in the always-on era requires more than recalibration of COPPA. It necessitates rethinking children's privacy in light of recent technology and offering proper safeguards for their protection under a more wholesome approach.

IV. RETHINKING CHILDREN'S PRIVACY IN THE ALWAYS-ON ERA

Many have argued that privacy is dead or that, at best, it deserves minimal protection in the digital age.[149] And even if privacy still exists—as another approach will argue—it is merely a currency, tradeable for services such as those provided to both adults and children by IoT devices.[150] Others might argue that the privacy implications of IoT are rising due to *media panic*,[151] *i.e.*, over-panicking about the perceived dangers of the use of new media by children that one finds unfamiliar and threatening.[152] If one accepts such approaches and their likes, then one might suggest that regulators should not bother protecting online privacy at all, including in regard to IoT devices. But even those who are skeptical of the need to protect privacy would not likely hold such a position regarding vulnerable members of society that are in need of greater protection, such as young children. The importance of protecting children's rights due to IoT technology increases as society is potentially entering an always-on era. They are constantly living within an environment, both in the public and private spheres,

148. Some have dubbed this era as that of "liquid surveillance", *i.e.*, as "modern societies seem so fluid that it makes sense to think of them being in a 'liquid' phase." ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE: A CONVERSATION vi (2013).

149. Scott McNealy, chief executive officer of Sun Microsystems, is famously quoted suggesting that "You have zero privacy anyway . . . Get over it." Polly Sprenger, *Sun on Privacy: 'Get Over it'*, WIRED (Jan. 26, 1999, 12:00 PM), 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, 1538–39 (2000).

150. *See, e.g.*, James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 14–17 (2005).

151. *See generally* Kirsten Drotner, *Dangerous Media? Panic Discourses and Dilemmas of Modernity*, 35 PAEDAGOGICA HISTORICA 593, 593 (1999).

152. *See* Michael Z. Newman, *Children of the '80s Never Fear: Video Games Did Not Ruin Your Life*, SMITHSONIAN MAG. (May 25, 2017), https://www.smithsonianmag.com/history/children-80s-never-fear-video-games-did-not-ruin-your-life-180963452/#aLUAvkSrMsR8ibwR.99.

that is packed with various sensors—many of them operating in either an always-ready or an always-on mode.

Children could not escape this era even if they wanted to. If children's privacy still matters—and under the current regulatory approach it does—then the framework that governs such protection is obsolete and ill-suited in an always-on era where their personal data could constantly be compromised. Even upon modifications and recalibration, COPPA will only properly regulate IoToys and few IoT devices, at best.[153] Even then, regulating merely IoToys will not advance the rationale of protecting children's privacy largely, realizing their potential exposure to IoT in their daily lives. Thus, as this part further shows, the regulatory framework that should have protected children's privacy in the past is inadequate to protect them in the always-on era. Without an overall regulatory change in the protection of privacy rights, this era might necessitate the use of other modalities of behavior regulation—with or without the law—but should remain constantly on policy-makers' agendas, as new technologies might threaten children's privacy even more in the near future. To properly address the challenges of the always-on era, the first subpart will reevaluate the sectoral approach to privacy generally, while arguing that it is ill-suited to properly safeguard children from IoT risks. The two other subparts then discuss non-legal modalities such as the market, social norms, and technology, which could aid in offering such protection; and further raise dilemmas on parenting and the future of children's privacy in the always-on era.

153. For more on how to recalibrate COPPA to meet the challenges of IoToys devices, see Haber, *supra* note 89, at 453.

A. Sectoral Smartification

The American approach to protecting privacy at the federal level, known as a sectoral approach to privacy, is inherently controversial.[154] Many scholars argued against such regulatory framework to protect privacy, and for the need to embrace an omnibus approach much like the European Union ("EU") has[155]—an overarching commitment to privacy that will guide all regulation and rule-making and could cover both the private and public sectors.[156] When considering the sectoral approach in the context of this Article, protecting data only under specific sectors, simply due to the potential increased probability that such data will be sensitive, seems rather redundant considering that OSPs could equally, and perhaps even more substantially, collect such data from children under the age of thirteen without falling under regulatory obligations.

COPPA could have provided proper protection for children's privacy rights, as it is generally designed to increase protection by using various fair information practices. As mentioned, it does provide some form of protection for those IoT devices that are clearly directed at children, like IoToys devices or the Echo Dot Kids Edition. This form of protection, while still in great need of modification and recalibration,[157] generally could aid in the protection of many children from

154. A sectoral approach generally means that data protection is regulated only within a specific context of information gathering or use, and it is usually directed only to specific, predefined industries or a specific cohort. Apart from COPPA, examples of such an approach could be found in various federal statutes, like that of the Financial Services Modernization Act (Gramm-Leach-Bliley) Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.) (generally regulating the personal information processing by financial institutions concerning the collection, use and disclosure of personally identifiable financial information); The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at 42 U.S.C. § 201) (regulating the privacy of health records by mandating the Secretary of the Department of Health and Human Services ("HHS") to promulgate rules for the manners in which states must protect the privacy of certain health information); Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. §§ 2710–2711 (2018) (regulating the use of video rental information and generally prohibits "video tape service providers" from disclosing personally identifiable information about their customers to a third party regarding rent or sale of video material.); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2794 (codified as amended at 47 U.S.C. § 551 (2018)) (requiring cable companies to maintain the confidentiality of cable subscriber's records); Right to Financial Privacy Act (RFPA), Pub. L. No. 95-630, 92 Stat. 364 (1978) (codified at 12 U.S.C. §§ 3401–22 (2018)) (setting limitations on financial institutions' disclosure of financial records to a government authority without a warrant or subpoena); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571-72 (1974) (codified as amended, 20 U.S.C. §1232g et seq.) (protecting the privacy of school records by regulating access to educational records, students' private records, and other information maintained by educational institutes, such as health records, psychological evaluations and other information directly related to the student); and the Fair Credit Reporting Act of 1970 (FCRA), Pub. L. No. 91–508, 84 Stat. 1114 (1970) (codified at 12 U.S.C. § 1830) (regulating the use of credit reports).

155. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1764 (2010); Solove, *supra* note 90; *cf.* Paul M. Schwartz, *Preemption and Privacy*, 18 YALE L.J. 904 (2009) (discussing the drawbacks of embracing an omnibus privacy regime). Notably, the FTC also issued a report and testified before Congress calling for baseline federal privacy legislation. *See The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. On Commerce, Science & Transportation*, 112th Cong. 1 (2012) (statement of Jon Leibowitz, Chairman, FTC), https://www.govinfo.gov/content/pkg/CHRG-112shrg81793/html/CHRG-112shrg81793.htm.

156. For more on omnibus versus sectoral approaches to privacy, see NISSENBAUM, *supra* note 88, at 237–38; Solove, *supra* note 90.

157. *See* Haber, *supra* note 89, at 431.

various online risks, and mostly that of datafication. This form of regulation is essential, as there is a high probability that many OSPs could collect personal information on children via these devices and misuse it, lacking sufficient incentives to refrain from doing so.

If the problem were merely children-targeted devices, then perhaps the sectoral approach would have provided adequate privacy protection, at least to some extent, as long as it was revisited, revised, recalibrated, and frequently updated to accommodate the differences of IoT from the internet. Furthermore, if the problem were to arise only from IoT devices that target children under the age of thirteen, then some regulators would have even been able to tackle this conundrum by taking rather extreme steps like banning the sale or even use of these devices overall—or at least specific devices that are more prone to privacy risks.[158] This radical approach, however, is not generally desirable for various reasons. For one, it will negatively affect the many benefits that are entailed in this technology, as IoToys and children-targeted devices can do more than merely enable new games or make old ones more accessible and enjoyable.[159] For instance, they could potentially assist in the overall education and cognitive development of children.[160] Aside from potential drawbacks of such a move, like its negative impact on innovation and other benefits that IoT entails, this solution will disregard children's right to participate freely in cultural life and the arts.[161] Evidently, these toys might also be important from the viewpoint of innovation and the improvement of technology.

But as mentioned, the problem extends far beyond children-targeted devices. Focusing merely on devices that have a higher probability of data collection, while important, could become somewhat meaningless in light of the smartification trend, by which the use of IoT devices is constantly on the rise.[162] It fails to acknowledge the move towards an always-on era, by which public and private infrastructure greatly depend on IoT. Beyond the smartification of our houses, state officials are likely to embrace smart infrastructure such as roads

158. Banning at least some IoToys was recently chosen by German authorities, deciding to ban the IoToy Cayla due to its security flaws, and to classify Cayla as an illegal, unlicensed radio device, meaning that parents who possess this doll might be prosecuted and face up to two years imprisonment for possessing a banned surveillance device. Similarly, Germany also recently banned children's smartwatches. *See* Dakshayani Shankar*, Germany Bans Talking Doll Cayla over Security, Hacking Fears*, NBC NEWS (Feb. 18, 2017, 6:43 PM), http://www.nbcnews.com/news/world/germany-bans-talking-doll-cayla-over-security-hacking-fears-n722816*;* Jane Wakefield, *Germany Bans Children's Smartwatches*, BBC NEWS (Nov. 17, 2017), http://www.bbc.com/news/technology-42030109.

159. These toys and devices could, for instance, carry educational and social benefits for children. For more on the benefits of IoToys devices, see STÉPHANE CHAUDRON ET AL., KALEIDOSCOPE ON THE INTERNET OF TOYS: SAFETY, SECURITY, PRIVACY AND SOCIETAL INSIGHTS, 9 (2017), http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf. Notably, however, these toys had also been criticized by many as they could provide poor quality of play, potentially harming children's development and impeding child-parent interaction, obstructing children's well-being and healthy development, and pose a health risk from electromagnetic radiation ("EMR"). For these arguments, see Haber, *supra* note 89, at 407–08.

160. *See* Children's Connected Toys, *supra* note 78, at 17.

161. Children's right of participation is formally acknowledged under the United Nations Convention on the Rights of the Child. *See* Convention on the Rights of the Child, art. 31, Nov. 20, 1989, 1577 U.N.T.S. 3.

162. *See* Columbus, *supra* note 69.

and cities. In the near future, many parts of the world, both public and private, will most likely become hyper-connected to the internet, constantly collecting and sharing data.[163]

But even prior to a total smartification of this world, the fact that children are datafied within their domestic surroundings must reignite the discussion on sectoral privacy. Children's privacy in the always-on era could serve as an example of how sectoral privacy could be ill-suited to protect the values which it was designed to protect. Children's privacy will not be easily protected without adhering to an omnibus approach, as it would be either implausible to exclude their datamining or introduce more intrusive ways of data analysis that will further downgrade everyone's privacy. This smart world could not coexist with the current regulatory framework that governs children's privacy. The examples of how COPPA poorly protects children's privacy within the IoT might broadly reflect on the applicability of the sectoral approach to protect privacy. Thus, if policy-makers consider that children's informational privacy deserves protection, then the always-on era necessitates an omnibus approach which will increase privacy protection for all individuals, including children, while still setting higher standards for those interactions which clearly include children's personal data.

Normative arguments, however, are not always translated into pragmatic solutions—or at least feasible ones. It is currently unlikely that policy-makers will easily abandon their approach to informational privacy, even upon acknowledging the potential challenges that the sectoral privacy approach entails. Even without an omnibus approach to privacy for all sensitive forms of data, policy-makers could, in the very least, regulate IoT within the sectoral approach by expanding the scope of COPPA. To do so, they must first acknowledge that regulating IoToys will be insufficient to properly protect children in the always-on era, and subject at least some IoT devices to the regulatory framework of COPPA. They must acknowledge that in this era, many children cannot simply opt out. Children are part of this world, and their data will be mined through private companies. They might not be allowed to use certain devices but will be dependent on others, simply to grab food from the refrigerator, make themselves a toast, or turn on the TV. Thus, apart from those devices, like IoToys that are already regulated under COPPA, it would be wise to differentiate between the potential use by children and the necessity to use IoT devices, along with the specific datamining capabilities of such devices. Smart toasters might not raise similar privacy concerns like smart TVs, and thus, even if both are not directed at children nor knowingly collect data from them, smart TVs might necessitate imposing different legal obligations than those imposed on IoT toasters.

But it is not merely a matter of necessity. Children under the age of thirteen might be surrounded by always-on devices that constantly monitor and datafy them. With the potential smartification of almost everything, there will be little escape from datamining. Policy-makers must thus oblige IoT OSPs to apply similar safeguards for devices that children might use within their houses if these are

163. *See* SCHNEIER, *supra* note 75, at 3–10.

capable of collecting personal information from them. This becomes more evident for those offering always-on services, which must be COPPA-compliant as a default, unless upon examination of their use, the regulatory framework had set strict terms for their exclusion.

This problem obviously extends far beyond children's privacy. The move towards an always-on society effectively means that the protection of those types of data that were once regulated by the sectoral approach might not work any longer. If, for instance, health information was once perceived to be handled mostly by hospitals and medical institutions, IoT, and perhaps most significantly fitness wearables, might divulge much of this data, and lacking direct regulation, it will be difficult to protect the privacy interests of individuals.[164] Perhaps eventually, American policy-makers will reconsider a wholesome approach to data privacy protection and not merely a sectoral one, to more adequately protect individuals' rights.[165] But until then, one might suggest that perhaps regulation under the sectoral approach is not the only form to properly protect individuals from privacy harms. Perhaps the use of other modalities, such as that of social norms, the market, and technology, will provide better safeguards for children's datafication—with or without regulatory intervention—while not yet forsaking the sectoral approach altogether.

B. Children's Privacy and Non-legal Modalities

The EU is generally considered one of the worldwide leaders in terms of data protection, especially upon the passage of the comprehensive General Data Protection Regulation ("GDPR").[166] Notably, however, the GDPR is far from

164. The Health Insurance Portability and Accountability Act of 1996 (HIPPA) applies to individually identifiable health information held by covered entities or business associates, and requires, *inter alia*, various forms of protections and affirmative consumer consent for certain uses. *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996); HIPAA Privacy Rule, 45 C.F.R. § 164.514(b)–(c) (2019); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach-Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pt. 160–64). For more on the HIPAA rule, see Frank Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 7 STAN. TECH. L. REV. 595, 608–20 (2014); Jennifer Glasgow, *Defining 'Sensitive' in World of Consumer Data,* ACXIOM (July 27, 2015), https://www.acxiom.com/blog/defining-sensitive-world-consumer-data.

165. For more on various proposals or recommendations regarding a U.S. federal data privacy law, see ALAN MCQUINN & DANIEL CASTRO, A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA, 3–5 (Jan. 2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf?_ga=2.133508621.2608225.1547562460-907254814.1547562460.

166. While the GDPR protects all data subjects within the EU and the European Economic Area ("EEA"), it also sets higher standards for all collection, use and disclosure of data when children's data are sometimes involved. Article 8 sets a parental consent requirement for all children aged under sixteen where online services are offered directly to them; while EU member states can lower the age threshold to thirteen. Consequently, Recital 38 requires prior parental consent before processing children's personal data. *See* Commission Regulation 2016/679 of Apr. 27, 2016, 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 further reading on the EU's perception of protecting children's privacy, see generally Sonia Livingstone, *Children: A Special Case for Privacy?*, 46 INTERMEDIA 18 (2018); Milda Macenaite, *From Universal Towards Child-*

perfect, and it has also received a fair amount of criticism on various grounds.[167] Without adhering to an omnibus approach as reflected by the GDPR, perhaps the protection of children should rely less on regulation and more on other modalities of regulating behavior, like that of the market, social norms, and technology, either separately or combined.[168]

Both the *market and social norms* could potentially reduce the privacy risks of IoT to children. Such a scheme would rely mainly on consumer discontent with the practices that IoT manufacturers engage in which risk their children's privacy. Under this approach, upon proper understanding of privacy risks, many, if not most, individuals might choose to at least abstain from purchasing devices that might pose a risk to their children.[169] This will not be exclusive to IoToys devices, but rather to smart devices in their homes or otherwise in the vicinity of children, at least those that are embedded with sensors that are capable of obtaining sensitive data. Consumers will either not purchase IoT devices that do not meet their expectations or drive competitors to meet them. In turn, companies might deploy various self-measures that would meet such expectations and eventually lead to better protection of children's privacy.[170] These measures could take many forms and are likely to be combined with the modality of *technology*.

Technology could embed privacy into the underlying specification or architecture of the IoT device and data gathering, *i.e.*, use a Privacy-by-Design approach.[171] One measure would rely on the *use of data* by companies and third parties. Upon consumers' demand, IoT OSPs could either cease data collection altogether, store data only locally on the device itself, embrace a data minimization approach, or avoid sharing data with third parties, to name but a few examples. But eliminating, and perhaps even reducing, data collection is highly improbable for most OSPs. Data is generally highly valuable for most companies for a variety of business and operational purposes.[172] Datafication could be essential for developing technology, for analysis, and "business models to utilize the derived information."[173] It could also be essential for the improvement, and

Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation, 19 NEW MEDIA & SOC. 765 (2017).

167. *See, e.g.*, Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995 (2017) (arguing that four central concepts of EU data protection law as manifested in the GDPR are incompatible with the prospects of Big Data analysis); *cf.* Daniel Solove, *Why I Love the GDPR: 10 Reasons*, TEACHPRIVACY (May 2, 2018), https://teachprivacy.com/why-i-love-the-gdpr ("The GDPR is the most profound privacy law of our generation.").

168. As suggested by Lawrence Lessig, there are 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: THE NATURE AND FUTURE OF CREATIVITY 116–73 (2004).

169. *See* Lawrence Lessig, Code: Version 2.0 129–37 (2006).

170. Apple, for instance, recently announced that they plan to change the rules it has for kids' apps to allegedly "better protect users' privacy by shielding children from data trackers." *See* Reed Albergotti & Craig Timberg, *Apple Aims to Protect Kids' Privacy. App Makers Say It Could Devastate Their Businesses*, WASH. POST (Aug. 20, 2019, 5:00 AM), https://www.washingtonpost.com/technology/2019/08/20/apple-aims-protect-kids-privacy-app-makers-say-it-could-devastate-their-businesses.

171. *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1411–12 (2011).

172. *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, 537 (2005).

173. *See* Tal Z. Zarsky, *The Privacy-Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 118 (2015).

even functioning, of the services provided, and even vital to advancing knowledge, innovation, and the development of machine learning, deep learning, and big data analysis, among others.[174]

Another technological measure would be increasing the *security of devices*, including that of their communication and of the stored data. Generally speaking, implementing various forms of security measures could ensure, or at least substantially reduce, misuse of the data and the ability to hack into the databases that possess the information.[175] Manufacturers could, for instance, use encryption methods to ensure only authorized access to the data gathered. While important for both adults and children, this solution is only a partial one, as it might reduce the potential misuse of the data by various parties but will not aid much in the datafication of children by the operating OSP.

But data security as a potential panacea for datafication is not limited to unauthorized access. OSPs can implement various techniques that would, at the very least, reduce privacy risks to children by disconnecting the data subject from the data. While using methods like data anonymization could prove as problematic,[176] other methods, like differential privacy,[177] or homomorphic encryption,[178] could aid as part of a solution. Others might argue against these potential solutions as their implementation might, *inter alia*, produce inaccurate outcomes

174. *See, e.g.*, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, FTC 21 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter Privacy & Security in a Connected World] ("Requiring fledgling companies to predict what data they should minimize would 'chok[e] off potential benefits and innovation.'"); Yuji Roh, Geon Heo & Steven Euijong Whang, *A Survey on Data Collection for Machine Learning: A Big Data-AI Integration Perspective*, ARXIV (Aug. 12, 2019), https://arxiv.org/pdf/1811.03402.pdf.

175. See, for instance, in California, whereas beginning in January 1st, 2020, IoT devices will be required to have "reasonable" security features. Adi Robertson, *California Just Became the First State with an Internet of Things Cybersecurity Law*, VERGE (Sept. 28, 2018, 6:07 PM), https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

176. While anonymization could generally increase privacy interests of individuals, researches have proven that many times adversaries could use reidentification or deanonymization methods to discover the identity of the data subjects. *See generally* Andrew Chin & Anne Klinefelter, *Differential Privacy as a Response to the Reidentification Threat: The Facebook Advertiser Case Study*, 90 N.C. L. REV. 1417, 1417–28 (2012); Ohm, *supra* note 155; Andreas Haeberlen, Benjamin C. Pierce & Arjun Narayan, *Differential Privacy Under Fire, in* PROCEEDINGS OF THE 20TH USENIX SECURITY SYMPOSIUM 1 (Aug. 2011), http://www.cis.upenn.edu/~ahae/papers/fuzz-sec2011.pdf.

177. Differential privacy is a standard which strives to assure that presence or absence of an individual in a dataset does not make significant difference to an outcome of any given database query, while introducing "noise" to the data. It strives to mathematically ensures that reidentification will be almost impossible, and that individuals' data could remain in the database without anyone knowing that it exists. For more on differential privacy, see, for example, Jane Bambauer et al., *Fool's Gold: An Illustrated Critique of Differential Privacy*, 16 VAND. J. ENT. & TECH. L. 701, 712–17 (2014); Cynthia Dwork et al., *Calibrating Noise to Sensitivity in Private Data Analysis*, *in* PROCEEDINGS OF THE 3RD CONFERENCE ON THE THEORY OF CRYPTOGRAPHY 265 (2006); Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1139–40 (2013); Chin & Klinefelter, *supra* note 176, at 1430, 1452–54; Ohm, *supra* note 155, at 1756.

178. Homomorphic encryption generally enables computations on encrypted data without needing to first decrypt the data. For more on this method, see David J. Wu, *Fully Homomorphic Encryption: Cryptography's Holy Grail*, 21 ACM MAGAZINE FOR STUDENTS 24 (2015).

for OSPs, prove to be costly and difficult to implement, or bring chaos to database systems.[179]

OSPs could even use technological measures that rely on implementing features like voice or facial recognition that could aid in reducing privacy risks, *i.e.*, that the IoT device will only operate for eligible users. Under this assumption, caregivers could allow their under-thirteen-year-olds to use the smart toaster but not use Amazon Echo. They could also enable children to use specific features in the Amazon Echo that do not greatly risk their privacy, while being restricted against using others. Even if technologically possible, the main problem with this solution, however, lies within the collection of biometric identification. This form of personal identifiable information could be misused by third parties, like hackers, and hence is not necessarily desired.

Restricting or limiting interactions of children under the age of thirteen with IoT technologies could be arranged without biometric identification. As long as the OSP enables such features, caregivers could set limitations on the use of IoT devices by children while also granting parental control on their datafication. Use limitations could include passwords, which would theoretically ensure the use of a device only by an authorized individual. Under such a parental control solution, and much like COPPA obligations, caregivers would be granted the ability to access, view, and delete the data that is acquired by all IoT devices and thus be in control of their children's datafication.[180]

There could also be other examples of imposing restrictions or limitations. One would be physically disabling children's access by various measures. Amazon Echo, for example, allows users to disable the "always listening" microphone by physically pressing a mute button on the top of the device.[181] Even if OSPs do not provide convenient ways to disable IoT devices, caregivers could disable data collection by turning them off or unplugging them when not in use or when children are present.

The problem, however, is that setting limitations would be impractical for many IoT devices. Implementing such childproof features in IoT, and mainly always-on devices, will defeat much of the automation rationales that are embedded in such technology—designed, *inter alia*, to preform and enable daily

179. Many scholars have argued that introducing noise has limited benefit in the use of data. *See, e.g.*, Bambauer et al., *supra* note 177, at 704; Ohm, *supra* note 155, at 1757; *see also* Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security Myths and Fallacies of "Personally Identifiable Information*," 53 COMM. ACM 24, 26 (June 2010), http://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf.

180. *See* 15 U.S.C. § 6502(b)(1) (2018). It should be further noted that while more general in nature, the Due Process Clause of the Fourteenth Amendment also grants parents the right to make decisions regarding the "care, custody, and control of their children." *See* U.S. CONST. amend. XIV.

181. *See* Gary Robbins, *Tips on Protecting Your Privacy on Amazon Echo and Google Home*, SAN DIEGO UNION-TRIBUNE (Jan. 5, 2017, 4:03 PM), https://www.sandiegouniontribune.com/news/science/sd-me-echo-home-20170105-story.html.

tasks in a convenient way.[182] Aside from the fact that children might learn passwords, setting them for every use of an individual's TV, Amazon Echo, or any other device will greatly defeat the convenience factor behind using them.[183]

Aside from the various social and psychological aspects that parental control could entail,[184] it would be highly impractical for caregivers to be in control of the data acquired by all their IoT devices.[185] Consider an always-on device that captures data 24/7. Caregivers will not have the ability nor the time to keep track of and sift through all the recordings of their children from all available devices. This solution might only be viable if the collector could alert caregivers, at least when a high magnitude of probability that the obtained data is that of a child under the age of thirteen exists. But even then, it would be implausible for caregivers to monitor all the devices in their households.

At this point, one could suggest that technology might offer solutions for better protecting children's privacy. Whether the market or social norms will effectively lead to such solutions is debatable. While a libertarian approach that relies on market forces sounds optimal not merely due to its associated freedom but even simply because it reduces regulatory costs, in practice it might not work. It will require the market to offer good substitutes with higher informational privacy protection and expect consumers to use only IoT devices that satisfy their demands. Unfortunately, this solution is not feasible, due to several market failures that prevent the market from optimal self-regulation.

One of these market failures occurs due to information gaps, cognitive failures, and structural problems. Generally, changing social norms regarding the use of IoT devices will be difficult. It first requires awareness to the risks that these devices entail. Without legal intervention, market players are underincentivized to disclose the potential risks that these devices pose, as it could potentially alienate customers. Obviously, however, it would be wrong to assume that market players will always prefer not to disclose any information on their products or services. Nondisclosure of relevant information could lead to mistrust and even legal actions based upon harm, even without specific regulation like COPPA.[186] Still, the market lacks the necessary incentives to fully disclose the risks of IoT devices to children.

And even upon the disclosure of such practices, which are usually communicated through privacy policies, ToS agreements, or EULAs, most end users

182. *See* Insights Team, *A Day in the Life Of Ms. Smith: How IoT and IIoT Enhance Our Lives*, FORBES (Oct. 11, 2018, 11:21 AM), https://www.forbes.com/sites/insights-inteliot/2018/10/11/a-day-in-the-life-of-ms-smith-how-iot-and-iiot-enhance-our-lives/#41a4bc2917ab.

183. *See* Privacy & Security in a Connected World, *supra* note 174, at 22 ("[I]f patients have 'to consent to everything' for a health monitoring app, 'patients will throw the bloody thing away.'").

184. *See generally* Bernstein & Triger, *supra* note 45.

185. Many IoT devices indeed offer such form of control over the data that is captured and recorded. Amazon, for instance, enables deletion of old recordings and the search history from its Echo devices, not only for children's data. *See* Robbins, *supra* note 181.

186. Privacy & Security in a Connected World, *supra* note 174, at 51 ("Consumers are more likely to buy connected devices if they feel that their information is adequately protected.").

will not bother reading them, as they are usually long and written in a legal language almost incomprehensible to most people.[187] Even upon knowledge and understanding of these practices, caregivers might simply not understand the privacy implications of such data collection and retention, and thus fail to act against it. Even adhering to a notice-choice mechanism, much like what exists under COPPA,[188] might prove burdensome both for the company and the consumer, and most importantly, ineffective to protect privacy.[189]

Moreover, this difficulty is enhanced due to reliance on rational choice theory, based upon the concept that well-informed and skilled individuals make rational decisions.[190] Truly, the notion of privacy as a concept of the self as inherently autonomous entails that the liberal self will possess the right of rational deliberation and choice.[191] Even so, a rational player might not easily forsake an IoT device due to its datamining policy, even if he or she understands the complex aspects of informational privacy. Many have a digital appetite that must be satisfied, while others might weigh in other factors, like convenience, when making these decisions.

Another difficulty is that of competition. The market must be competitive enough to provide substitute goods. If the market is monopolistic or oligopolistic in nature, parents might not have alternatives to choose from. Taking IoToys as an example, this market is largely controlled by huge toy conglomerates, like Mattel.[192] These toys could not be deemed as substitute goods, as the manufacturer operates in a monopolistic competition. Hence, without valid alternatives

187. For more on this issue, see Annie I. Antón et al., *The Lack of Clarity in Financial Privacy Policies and the Need for Standardization*, 2 IEEE SECURITY & PRIVACY 36, 44–46 (2003); Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546 (2014) ("Consumers seldom read the form contracts that firms offer."); Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 665–78 (2011); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 544 (2008); George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15, 20–21 (2004); Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1885 (2013); Aaron Smith, *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.

188. Much of the discussion on the protection of children's privacy revolves around the role of caregivers to protect their children from risks and harms. COPPA itself relies on this rationale to a great extent, providing caregivers the right—and subsequently, the obligation—to choose whether their child will be datafied, and what companies could eventually do with the gathered data. This could be learned, *inter alia*, from COPPA's notice, consent, and data minimization requirements, and from the right to refuse further use or maintenance or future online collection of personal information from that child and to obtain such data. *See* 15 U.S.C. §§ 6502(b)(1)(A)–(B) (2018); 16 C.F.R. §§ 312.4–6 (2018).

189. *See* Privacy & Security in a Connected World, *supra* note 174, at 22 ("[I]t would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.").

190. For a detailed analysis of rationality, see generally ROBERT NOZICK, THE NATURE OF RATIONALITY (1993); Russell B. Korobkin & Thomas S. Ulen, *Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics*, 88 CALIF. L. REV. 1051, 1060–66 (2000).

191. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1907 (2013).

192. For more on Mattel's market share, see Shoshanna Delventhal, *A Tale of Two Toy Makers: Mattel and Hasbro*, INVESTOPIA (July 25, 2019), https://www.investopedia.com/news/tale-two-toy-makers-mattel-and-hasbro.

that better protect their child's privacy, many parents might give in to purchasing the toy. Even if we assume that the IoToys market operates in a perfect competition mode, it might be perceived as a market that could not enable substitute goods to begin with. But even assuming that social norms dictate it, OSPs might not be fully motivated to provide protection for their consumers. Even if OSPs adhere to consumers' expectations, they might still act irrationally, lured by short-term gains, and might simply fail to acknowledge the benefits of protecting their customers.[193]

Aside from the abovementioned difficulties, so long as data remains highly valuable for companies, it is unlikely that they would set barriers for its collection. Notably, data is also highly valuable from a governmental angle. The state has an interest in the data acquired by IoT devices—including that of children.[194] If, by now, we have already learned that governments, like that of the U.S., had partnered with many technology companies to obtain information that was transmitted in their networks (upstream collection), then it is evident that IoT devices, especially those that operate in an always-on mode, are a goldmine for governments.[195] As we learned from Edward Snowden's revelations, there is a valid chance that enforcement agencies could also—and perhaps already—have access to such information.[196] They could obtain such data using the legal framework that governs stored communications, or perhaps even obtain it directly from private companies through what is commonly termed as a Public-Private Partnership.[197] Thus, any restrictions on data collection—or even the use of encryption—might face governmental opposition, which in turn could compel OSPs to not adhere to such measures, either formally by regulation or informally by various means.[198]

Despite their difficulties, non-legal modalities should still play an important part in protecting children's privacy. But lacking direct regulation, it is improbable that they will properly protect children from datafication that occurs from IoT devices. Thus, without revolutionizing the concept of privacy in the U.S., the future of children's privacy becomes blurry, as the always-on era might continue to expand, posing further risks and harms. But along with such regulation, one might suggest that the current state also necessitates parental intervention—focusing on the role of caregivers to protect their children, even lacking legal or technological intervention. In other words, while regulation might be crucial at this stage, parenting in the always-on era might also require adjustments to these new technological changes.

193. *See* Zarsky, *supra* note 173, at 131.

194. *See* Lupton & Williamson, *supra* note 45, at 4.

195. *See id.* at 3

196. *See id.*

197. Arguably, it could trigger constitutional rights like that of privacy as set under the Fourth Amendment, which protects against unreasonable searches and seizures. *See* U.S. CONST. amend. IV. Currently, however, it would seem that the third-party doctrine will prevail, and companies will not be held accountable for any disclosed data to the government. *See generally* Elkin-Koren & Haber, *supra* note 15.

198. Under public-private partnerships, some companies might be incentivized to voluntarily aid enforcement agencies for various reasons such as immunity or other benefits. For more on such public-private partnerships in a different context, see generally *id*.

C. Smart Parenting and Regulation

Protecting children's privacy in the always-on era necessitates some form of legal intervention. But, along with regulatory adjustments or even resorting to an overall approach to protect individuals' privacy regardless of age, educating children on the risks of IoT devices to their privacy is important. This is where parenting might become crucial. As parents have both the right and responsibility to protect their children and to make decisions regarding the "care, custody, and control of their children" in the offline world, similar responsibilities arise from the always-on era.[199]

Thus, one might argue that the solution to such conundrum lies on the caregivers. Under this approach, caregivers should, for instance, educate their children on the use of IoT devices that might collect and retain personal data, and refrain from using devices that do not properly safeguard their rights. They could, for instance, restrict or limit their children's interactions with devices that might collect sensitive data, but permit the use of those which do not. Caregivers could also allow the use of some IoT devices only when they are present, and limit or restrict it otherwise. Essentially, much like they educate their children on any risks that they might encounter in their daily routine, caregivers should aid in the overall digital education of their children.

While digital education is important regardless of this Article's scope, the problems of knowledge, expertise, and the functioning of these devices—that might be always-on regardless of actual use, for instance—might raise a barrier to education. While parents are accustomed to guarding their children from risks that might arise from television and other familiar media, the internet might result in a "regulation gap" between parental willingness and parental competence.[200] Adding the layer of IoT will further broaden such a gap. Thus, caregivers might lack the necessary knowledge and expertise to make such assessments on their children's privacy. Only upon closing such potential gaps could parents, to some extent, forbid their child from using an IoT device—at least until the child reaches some level of maturity, similar to how parents educate their children in other aspects. Still, the always-on functionality will keep threatening children's privacy, even if it does so to a lesser extent.

Moreover, many caregivers might consider the privacy implications of IoT devices nondramatic, or even an integral component of living in a hyper-connected world. They might feel that it is not the law that needs to be adjusted, but rather society's expectations regarding their datafication—including their children's. Children's surveillance might, as mentioned, begin at very early stages of their lives, even prior to birth.[201] They grow up in a sensor-embedded reality that is constantly datafied. They might go to kindergartens or schools that are

199. *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. 65 (2000). For further reading 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, 977 (1988).

200. *See* Livingstone, *supra* note 41, at 52.

201. *See* Lupton & Williamson, *supra* note 45, at 4.

equipped with various sensors, like cameras and radio-frequency identification ("RFID") chips.[202] Thus, one might argue that children's monitoring is by now integral to their lives, leading to the normalization of surveillance of them.[203] This form of normalization could arguably aid children in entering the always-on era when they grow up, reducing any knowledge and expertise gaps that might occur when they are not exposed to this world. To continue this line of argument, datafication of children by constant monitoring and surveillance could actually aid in mitigating future gaps and prepare them better for adulthood.

Perhaps datafication and surveillance are not necessarily bad for children. They can make them feel safer, improve their skills, and generally optimize their lives.[204] When choosing to voluntarily participate in data-sharing practices, such as using social media platforms, they might contribute to processes of selfhood and identity, and aid them in self-improvement.[205] Perhaps most importantly in the context of children's rights, IoT could improve their ability to exercise their rights to information, education, and participation.[206]

But such datafication is highly problematic from many aspects, aside from privacy. If individuals are datafied almost from their conception, then algorithms will most likely make important assessments and judgements and thus control the trajectory of their lives.[207] And algorithms, as we know, can be flawed. The algorithm could contain mistakes and biases, among many other problems.[208] To that extent, without incentives to minimize the datafication of children and the storage of data, children's rights and liberties, as well as their well-being, might be at risk. Growing up in an always-on era without safeguards will lead to diminishing the values that privacy seeks to protect.

Thus, while smart parenting is crucial in this age, it still necessitates legal intervention. With the quick pace of technological innovation, regulators must consider the potential implications of new technologies and regulate them when necessary. If legal and social norms dictate protecting children from data abuse, then IoT devices, especially those directed at children, cannot be regulated through an obsolete statute that does not grant them proper protection. Children must not be treated as guinea pigs for the sake of innovation. It is not merely a personal privacy concern, but rather an important turning point in society in which regulators must decide on its core values. If society accepts the notion that

202. In the United Kingdom, for instance, many schools have CCTV cameras that track students, and many use radio-frequency identification chips in badges or school uniforms to track movements. *See generally* EMMELINE TAYLOR, SURVEILLANCE SCHOOLS: SECURITY, DISCIPLINE AND CONTROL IN CONTEMPORARY EDUCATION 22 (Martin Gill ed., 2013); Lupton & Williamson, *supra* note 45, at 6.

203. For more on the normalization of surveillance, see David Murakami Wood & C. William R. Webster, *Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example*, 5 J. CONTEMP. EUR. RES. 259, 262 (2009).

204. *See* Lupton & Williamson, *supra* note 45, at 8.

205. *Id.*

206. *See generally* Sonia Livingstone, *Reframing Media Effects in Terms of Children's Rights in the Digital Age*, 10 J. CHILD. & MEDIA 1, 9 (2016).

207. *See* Lupton & Williamson, *supra* note 45, at 2.

208. *See, e.g.*, Sandra G. Mayson, *Bias In, Bias Out*, 128 YALE L.J. 2218, 2275 (2019).

convenience always triumphs over our civil liberties, so be it. But such acceptance must be consensual with proper knowledge and education on the capabilities and use of always-on devices. Until we reach such an informed consent, regulators must place proper limitations on the manufacturing and use of technology, as innovative as it might be.

At the same time, policy-makers must generally be wary of heavily regulating IoT technology. Beyond economic efficiency and other benefits to society,[209] IoT technology, and more specifically voice-activated devices, could obviously improve the quality of life for many of their users.[210] To take full advantage of the technological capabilities, devices in the future could even analyze our voices and detect whether we are stressed (and analyze the source of such stress), or detect whenever we are in danger and contact emergency services like the police or anyone else we identified as such.[211] Moreover, addressing the challenges of IoT to privacy risks through specific legislation could be premature at this stage.[212]

All in all, if policy-makers do not adhere to an omnibus approach, and as long as other modalities like technology, social norms, and the market, are limited in solving the problem, COPPA must be broader. Even without its recalibration, simply acknowledging that the actual knowledge standard must change will be a good start. IoT companies must not be able to escape COPPA's framework under an "ignorance is bliss" approach. As mechanisms get smarter, so do their data analytics, meaning that in many instances they will possess the tools to know whether a child was datafied or not. If, for instance, a user communicates age identifying questions or answers to the IoT device, like the grade that she is currently in, then these IoT manufactures must adhere to COPPA framework.[213]

On a broader scale, the always-on era necessities rethinking the defaults of data collection from children. It is upon the OSP—not only the user—to actively question whether its services are in use by young children. But the responsibility must also lie on caregivers to communicate such data initially. To do so, privacy preferences regarding the use of some home devices by children should be easily set to be handled by users.[214] It would apply for all devices, thus eliminating the burden of configuring every device separately. Upon connecting to the caregiver's predefined characteristics, which could be embedded within an app or

209. Smart thermostats, for instance, can improve energy efficiency and thus promote social goals. *See* Children's Connected Toys, *supra* note 78, at 3.

210. Beyond making everyday tasks more convenient, this technology could potentially improve the lives of many individuals, like those with physical disabilities. *See* GRAY, *supra* note 26, at 6.

211. *See* David Talbot, *The Era of Ubiquitous Listening Dawns*, MIT TECH. REV. (Aug. 8, 2013), https://www.technologyreview.com/s/517801/the-era-of-ubiquitous-listening-dawns/.

212. *See* Privacy & Security in a Connected World, *supra* note 174, at 48–49.

213. The FTC clarifies that "An operator also may have actual knowledge based on answers to 'age identifying' questions like 'What grade are you in?' or 'What type of school do you go to? (a) elementary; (b) middle; (c) high school; (d) college.'" FTC, CHILDREN'S ONLINE PRIVACY PROTECTION RULE: NOT JUST FOR KIDS' SITES (Apr. 2013), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites (last visited May 27, 2020).

214. For a similar proposition regarding privacy preferences, see Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 653 (2015).

even upon connecting to your Wi-Fi, all IoT devices that operate under the domestic internet connection will be required to adhere to these preferences.

Naturally, it would be highly difficult, if not over presumptuous, to forecast the future of children's privacy in an always-on era. But with such uncertainty in mind, children's rights must not be waived due to technological developments, but rather further explored in light of them. While the importance of privacy protection of adults should not be disregarded even if the right to privacy is seemingly headed towards its demise, children could be highly vulnerable to these technological developments, and the potential consequences of these devices to their privacy deserve proper attention and scrutiny. If such an evaluation is not on the immediate agenda of policy-makers, then it might prove to be too late.

V. CONCLUSION

Protecting children from online datafication becomes a real challenge for policy-makers in the always-on era. Choosing a sectoral approach to data protection may have worked to some extent for websites, but it does little to advance the protection of children in IoT. When children are likely to grow up in a world awash with sensors, regulating only IoT devices that directly target children will merely account for a fraction of the data that is gathered by IoT service providers on children. In other words, the current regulatory framework, even upon recalibration, is ill-suited to properly protect children's privacy, and policy-makers must consider other regulatory mechanisms that will eventually protect children's privacy better.

The always-on era, however, should not lead to the demise of children's privacy. On the contrary, protecting children's privacy in the always-on era becomes more crucial, as they are likely to be subjected to more forms of datafication than ever before in history. Policy-makers must abandon the sectoral privacy approach, at least when it comes to children's privacy, and adopt an omnibus approach that will enable better protection for all individuals. Still, even without forsaking the sectoral privacy approach, other forces should also come into play. Caregivers, for instance, could take protective measures, while educating their children on the implications of being constantly under datafication and surveillance. Consumers should at least attempt to drive the market to enable better safeguards for their children's privacy, including their own. And finally, technology must play a role by implementing Privacy-by-Design mechanisms that will ensure innovation on the one hand, and consumer's privacy on the other. Only then will children be able to fully exercise their civil rights and liberties, and most significantly their right to privacy.