THE INVISIBLE, YET OMNIPRESENT EAR: THE INSUFFICIENCIES OF THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

SUZANNE KAUFMAN

I. INTRODUCTION

Speaking aloud when no one else is near is no longer considered strange when a smart speaker or device is around. These devices have incorporated themselves into homes where they are available to, and used by, children and adults.[1] While these speakers may appear to make one's life easier, their constant collection and storage of information poses dangers and threats, especially to children.[2] Children's submission of personal information to smart speakers mirrors the finding that children are entering personal information to websites in many ways when going online without their parents knowing or approving.[3] Given the current environment of the ever-expanding integration of technology into our lives, issues with children's information privacy continue to increase.

The Children's Online Privacy Protection Rule, COPPA ("the Act"), was intended to protect children's personal information from first parties, companies that directly collect the information from the individual. But the pervasive yet unanticipated role of

1. Greg Sterling, *Roughly 1 in 4 U.S. Adults Now Owns a Smart Speaker*, MARTECH (Jan. 9, 2020, 2:09 PM), https://marketingland.com/roughly-1-in-4-u-s-adults-now-owns-a-smart-speaker-according-to-new-report-273994 [https://perma.cc/FR8E-PVE9] (stating that about 60 million U.S. adults own at least one smart speaker).

2. *See* Sonia Livingstone, John Carr, & Jasmina Byrne, *One in Three: Internet Governance and Children's Rights*, UNICEF INNOCENTI DISCUSSION PAPERS No. 2016-01, 23 (2016) (listing both the risks and opportunities that the internet, including smart speakers, present); Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUSTON L. REV. 751, 755 (2009) ("No one can deny, though, that Internet use *is* something of a threat to young families.").

3. Lauren A. Matecki, *Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era*, 5 NW. J. OF L. AND SOC. POL'Y 369, 373 (2010) ("The FTC found that children who went online were submitting personal information to websites in a wide range of capacities without the knowledge or approval of their parents.").

third parties, companies that receive aggregated data that was previously collected from individuals, has increased the difficulty of COPPA application, threatening the security of children's personal information. There is a distinction to be drawn between third parties who collect a child's information solely to perform a function requested, such as processing payments, and third parties who collect a child's information for the purpose of exploiting it.[4]

COPPA was designed to heighten security measures for children under the age of 13 by giving parents more control of their children's personal information. Yet, the role of third parties in data collection and sharing subverts the missions of both stricter protection of children as well as greater parental control. Even when the first party collects personal information of children in compliance with COPPA, the third parties with whom that information can eventually be shared do not all comply with the regulation. The child's personal information that was protected becomes no more regulated than any other adult's personal information. This Note will look at the ability of first parties, specifically Google and Amazon, to undermine COPPA by sharing children's information with third parties who do not comply with the Act. It will analyze whether COPPA is sufficient in protecting children's privacy by looking at whether first parties comply with the regulation, and, even if they do, whether their compliance achieves the goals of COPPA based on third-party sharing. This question gets to the central issue of whether COPPA is sufficiently protecting children's information. The effectiveness of COPPA can guide further amendments and reforms to the Act in order to reach the socially optimal outcome so that it can better serve its purpose without imposing useless or unhelpful requirements on companies.

A. Internet History

The risks to children, as users of the internet, are connected to the history of the use of the internet. In the 1990s, the internet became a place of marketing, sales, and distribution of products and services.[5] As the internet increasingly attracted children, abuses of their personal information rose, demonstrating just how much personally identifiable information (PII) can be collected from a

4. As used in this paper, the term "third party" will refer only to the latter where the information is less secure and unprotected.

5. Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55 (2007).

seemingly innocuous product or service.[6] For example, Mattel's Hello Barbie records conversations and sends to a server not only those of the child who consented but also those of any other children who interact with the doll.[7] To illustrate the severity of these abuses, in July 1998, Senators Richard Bryan and John McCain introduced a bill, some of which was later incorporated into COPPA.[8]

B. The Problem

The problems created by children's use of the internet are similar, but not identical, to the problems created by children's use of smart speakers and devices. There are five main problems created by children's use of the internet. First, the internet competes with activities that are better for children's growth and development—such as physical exercise, homework, and face-to-face communication—showing the failure of reaching the socially optimal outcome.[9] These activities are especially important to children, who are still developing and learning at rapid rates as compared to adults. The socially optimal outcome in this situation would not only be for children's privacy to be protected but also for children to be able to use the internet in ways that enhance their growth rather than compete with it. The goal of regulations such as COPPA should be to better incentivize behavior that leads to that socially optimal outcome. Second, the internet inappropriately exposes children to sex, violence, hate, and advertising and marketing content because of children's vulnerability and lack of awareness of certain warning signs that adults have grown accustomed to looking for.[10] Not only does the internet therefore undermine parental val-

6. OECD, *Chapter 2. Children and Digital Technologies: Trends and Outcomes*, *in* EDUCATING 21ST CENTURY CHILDREN (Tracey Burns & Francesca Gottschalk eds., 2019) (ebook), https://www.oecd-ilibrary.org//sites/71b7058a-en/index.html?itemId=/content/component/71b7058a-en#section-d1e2428 [https://perma.cc/38E4-7BQD].

7. Alex B. Lipton, Note, *Privacy Protections for Secondary Users of Communications-Capturing Technologies*, 91 N.Y.U. L. REV. 396, 406 (2016) (quoting Mattel's Hello Barbie's privacy policy: "By allowing other people to use the Service via your account, you are confirming that you have the right to consent on their behalf to ToyTalk's collection, use and disclosure of their personal information as described below.").

8. *Children's Online Privacy Protection Act*, TECH LAW JOURNAL, http://www.techlawjournal.com/congress/privacy/Default.htm [https://perma.cc/PKH9-LZ5A].

9. Allen, *supra* note 2, at 755–56 (comparing the harms of internet use to those of television viewing or comic book reading).

10. As used here, "vulnerability" refers to children's lesser ability than adults to identify bad actors and foresee the consequences of their actions. *See id.* at 756

ues and authority, but it, third, compromises child welfare by introducing and facilitating criminality such as juvenile hackers, identity thieves, and viral agents.[11] Fourth, the risk to children extends to their families through the child's participation in e-commerce, releasing not only their own PII but also family financial information without fully comprehending the effects of sharing financial information over the internet.[12] Fifth, the internet accounts for a substantial amount of bullying (i.e., cyberbullying) and harassment of which children are common targets.[13]

When looking at the release of personal information in particular, the risks to children are heightened. Once information is disclosed, unauthorized users are enabled to access and misuse personal information.[14] This further increases the vulnerabilities that could be used to compromise personal information.[15] Each compromised network facilitates attacks on other connected systems.[16] Overall, collection of children's personal information creates risks to their personal and physical safety.[17]

Children are especially at risk from the dangers posed by the internet and collection of personal information because of their vulnerabilities in not recognizing the dangers of others having access to their personally identifiable information and in being less able to identify bad actors.[18] For example, information can be col-

("Neither filtering practices nor rating systems have become pervasive or effective enough to reduce the threat of inappropriate exposure to children.").

11. *Id.* at 757 (explaining this problem through the example of Jonathan Lebed: "This New Jersey youth capitalized on the anonymity of the Internet and the gullibility of greedy adults to earn $800,000 by trading stocks.").

12. *Id.* ("Children are often indifferent to the forms of informational privacy and data protection of concern to adults.").

13. Livingstone et al., *supra* note 2, at 23 ("[S]ome [children] are vulnerable, resulting in mental distress, self-harm or even suicide . . . . [T]hese risks undermine children's rights regarding identity, reputation, privacy and play as well as safety.").

14. F.T.C., Internet of Things: Privacy & Security in a Connected World 10 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/6XPU-3YLN].

15. *Id.* at 11.

16. *Id.* at 11–12. ("For example, a compromised IoT device could be used to launch a denial of service attack. Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks.").

17. *Id.* at 10–14.

18. Matecki, *supra* note 3, at 374 ("[A] child would be likely to disclose information to websites, but lack the developmental capacity to fully understand the

lected from children more immediately and with less difficulty than from adults because of "the ability of the online medium to circumvent the traditional gatekeeping role of the parent."[19]

To exemplify the dangers posed to children in particular, one can look to the creation and motivation behind the Infancy Law Doctrine.[20] The idea behind the Infancy Law Doctrine is that children's inexperience and inattention causes them to be targeted by sellers, so children should have more protection when entering agreements online.[21] Some believe that children and teenagers have become "the epicenter of American consumer culture."[22] A child who is over-confident in their technological expertise needs more protection; "[t]oday, a new generation of computer-savvy minors sits confidently in front of their computer screens fearlessly and effortlessly initiating a multitude of contracts in cyberspace."[23]

Children are also at risk of those dangers that all users face. There are three main risks identified for all users. First is the lack of participation in decisions about one's own information, and second, the lack of control since the data is being stored for unknown future purposes.[24] The third risk is that when one's information is released, the release can lead to one being watched and one's behaviors being constrained.[25] As Daniel Solove describes, "the secrecy paradigm" also contributes to the risks internet users face in that individuals want to keep their information secret from certain people.[26]

---

consequences of such disclosure, such as widespread dissemination to third party advertisers.").

19. *Id.* As will be explained later, COPPA was designed to alleviate some of the risks to children. *See infra* Part II(A). But as this Note will explore and explain, COPPA has been unsuccessful with regards to that goal. *See infra* Part III.

20. Victoria Slade, *The Infancy Defense in the Modern Contract Age: A Useful Vestige*, 34 U. SEATTLE L. REV. 613, 613 (2011) (describing how children and teenagers have become the "epicenter of American consumer culture" and how that leads to consequences not only for their own futures but also for the future of "our culture").

21. *Id.* at 619 ("Many areas of law recognize that minors do not have the same capacity for decision making as adults.").

22. *Id.* at 613.

23. *Id.* at 623 n.64.

24. DANIEL J. SOLOVE, THE DIGITAL PERSON 42 (Jack M. Balkin & Beth Simone Noveck eds., 2004).

25. *Id.*

26. *Id.* at 8 (defining "secrecy paradigm" as the way in which "privacy is invaded by uncovering one's hidden world, by surveillance, and by the disclosure of concealed information").

The effects of information being released, especially for children, are long-lasting. Given that there are few opportunities to challenge the inferences made by algorithmic calculations, information about oneself, even from a young age, may stick with that person for their lifetime.[27] That information can impact one's access to opportunities.[28]

This Note argues that COPPA does not sufficiently achieve its goal of protecting children. Part II of this paper will explain the background and history of COPPA to provide some context for the regulation. Part III will dive into two smart speakers, the Amazon Alexa and the Google Assistant to analyze whether, and to what extent, they directly comply with COPPA as first parties. Part IV will discuss how, even if Amazon and Google do comply as first parties, they share the information they collect via the smart speakers with third parties who might not comply with COPPA. Part V will provide some suggestions on how to proceed, with a focus on law and economics theory, where the reasoning for the suggestions centers around the benefits to the economy overall. Finally, Part VI will conclude.

II.
BACKGROUND AND HISTORY OF COPPA

A. COPPA's Purpose

COPPA was the first federal privacy law directly addressing the online and electronic realm.[29] The creation of the Act was driven by privacy concerns and potential online safety risks such as online predators getting power over children's PII and the other threats and risks discussed above.[30] COPPA forces parents to get involved with their child's use of the internet and disclosure of information. As children increasingly used the internet, marketing companies

27. Deborah Lupton & Ben Williamson, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, 19 NEW MEDIA & SOC'Y 780, 786 (2017) ("[People] often have little knowledge about how corporations are exploiting their personal details and using them to construct detailed profiles on people.").

28. *Id.* (explaining how the profiles corporations create on people can be "used for decisions about their access to employment, insurance, social welfare, special offers and credit").

29. SOLOVE, *supra* note 24, at 70 (listing various statutes that pertain to privacy).

30. Simone van der Hof, *I Agree. . .or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World*, 34 WIS. INT'L L.J. 409, 422 (2017) ("[P]otential online safety risks, such as (online) predators getting their hands on children's personal data, were also perceived as very worrisome."); *see supra* Part I(B).

compiled lists of their PII and behavioral data that was subsequently sold to third parties, furthering the release and lack of control over one's own information.[31]

The collection of PII from children online presented concerns about the "vulnerability of children," "the immediacy and ease with which information can be collected from them," and "the ability of the online medium to circumvent the traditional gatekeeping role of the parent."[32] The objectives of the law, as summarized by COPPA's co-sponsor Senator Richard Bryan, were to: (1) increase a parent or guardian's involvement in their child's online activities to protect the child's privacy in the online environment; (2) protect a child's safety when using services in which a child could publicly post their PII; (3) maintain security of children's PII collected online; and (4) limit the overall collection of children's PII, especially that collected without parental consent.[33]

One of the goals of COPPA was to reduce the increased risk to children that came with the increase of online marketing and advertising.[34] Those risks included predatory marketing, stalking or kidnapping, and other threats described above.[35] The idea was that parents should be a part of the decisions made by children since parents are ultimately responsible for their children's well-being and safety.[36] The goal of COPPA was not to add burdensome requirements on online operators; in fact, legislators believed that COPPA would not introduce significant obstacles that would inhibit innovation, economic growth, or children's access to learning opportunities online.[37]

---

31. van der Hof, *supra* note 30, at 422 ("[I]nvestigative reports demonstrated the ease with which mailing lists consisting of children's personal information could be obtained from marketing companies.").

32. Matecki, *supra* note 3, at 374.

33. *Id.* at 375–76 (describing how, overall, the Act "sought to address the FTC's concerns and requests in the Privacy Online report").

34. Allen, *supra* note 2, at 752 ("Supporters believed COPPA would reduce the risk of one class of harms posed by the new economy to children who use computers, namely, imprudent disclosures of personal information by children.").

35. Danah Boyd et al., *Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act'*, 16 FIRST MONDAY (Nov. 7, 2011), https://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075 [https://perma.cc/A8XG-B7TQ].

36. Allen, *supra* note 2, at 773 (explaining how the Supreme Court and Congress often side with parents who want to restrict their child's access to information and services).

37. Boyd et al., *supra* note 35, at 3.

B. COPPA's Requirements

1. 1998 Version

The Children's Online Privacy Protection Act (COPPA) was enacted by Congress and signed by President Clinton on October 21, 1998.[38] It became effective on April 21, 2000.[39] COPPA is codified in the U.S. Code in Title 15, Chapter 91.[40] Generally, COPPA requires notice, transparency, security, confidentiality safeguards, parental choice, and parental consent for data collection.[41]

The Act applies to websites and services targeted at children, defined as people under the age of thirteen, or general-audience operations when there is "actual knowledge" that it is collecting personal information from a child.[42] Whether something is "directed" at children depends on the operator's intent, as well as the language, images, and overall design.[43]

There are several requirements under the regulation aimed at protecting children's privacy and the collection of their PII. COPPA's main requirements are: (1) a clear and comprehensive privacy policy; (2) obtaining "verifiable parental consent" before collecting, using, or disclosing a child's PII; and (3) obtaining "verifiable parental consent" after the data processing practices have been changed in a material way.[44] To get consent, the operator must provide the parent with "a description of the specific types of personal information collected from the child by [the] operator,"

38. Elizabeth R. Purdy, *Child Online Protection Act of 1998 (1998)*, THE FIRST AMENDMENT ENCYCLOPEDIA (2009), https://www.mtsu.edu/first-amendment/article/1066/child-online-protection-act-of-1998 [https://perma.cc/SPU3-TTP7].

39. *Children's Online Privacy Protection Act COPPA*, NATIONAL CREDIT UNION ADMINISTRATION (July 2001), https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/childrens-online-privacy-protection-act-coppa [https://perma.cc/NM88-9YV4].

40. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06 (2000).

41. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 646–47 (2014) ("COPPA is broad, encompassing meaningful notice, transparency, and parental choice and consent requirements, as well as security and confidentiality safeguards.").

42. SOLOVE, *supra* note 24, at 70 (referencing language from the Act that specifies that the Act only applies to websites that know they are collecting information from children). General-audience operations are defined as sites and services directed at people aged 13 or older. *See* Claire Quinn, *Know Your Audience or Pay the Price*, PRIVO (Mar. 31, 2020), https://www.privo.com/blog/know-your-audience-or-pay-the-price [https://perma.cc/M4X5-MVRA].

43. Allen, *supra* note 2, at 760 ("The determination of whether a Web site is directed to children under thirteen is based not only on the intent of the Web site operator, but on the language, images, and overall design of the site as well.").

44. van der Hof, *supra* note 30, at 422-23.

"the opportunity at any time to refuse to permit the operator's further use or maintenance . . . of personal information from that child," and "a means that is reasonable . . . for the parent to obtain any personal information collected from that child."[45] Parents are given a substantial amount of power under COPPA, extending to the right to veto the ways in which their child's PII is collected, used by both first and third parties, and maintained.[46] Many of these requirements are more difficult to achieve.

While the language of COPPA did not explicitly include reference to recording of a child's voice within the original version of the regulation from 1998, the 2013 amendment to the legislation clarified that such information is also protected.[47] There is an exception to the protection of audio files containing children's voices when the audio is collected only to replace written words, such as using the dictation tool instead of typing out a word, so long as the audio is only stored for a short period of time and is used solely for that purpose.[48] That exception does not excuse the operator from providing clear notice of collection and use of audio files in its privacy policy.[49] Once the audio file collected contains any PII, then the exception no longer applies, and the regulations of COPPA must be adhered to.[50] It should be noted that the exception does not change anything else about the operator's compliance with COPPA.[51]

Some argue that COPPA does not apply to smart speakers because smart speakers are not "directed to children" as defined in

45. 15 U.S.C. § 6502(b)(1)(A)(i) (1998); *see also* Allen, *supra* note 2, at 763.

46. Allen, *supra* note 2, at 763 ("Under COPPA, parents are ascribed a powerful right to veto primary collection, primary use, secondary use, and even maintenance of data.").

47. *FTC Provides Additional Guidance on COPPA and Voice Recordings*, FED. TRADE COMM'N (Oct. 23, 2017), https://www.ftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings [https://perma.cc/DLD9-G4RF] (adding "video or audio file that contains a child's image or voice" to the definition of personal information); *see infra* Part II(B)(2).

48. *FTC Provides Additional Guidance on COPPA and Voice Recordings*, *supra* note 47 ("The FTC will not take an enforcement action against an operator for not obtaining parental consent before collecting the audio file with a child's voice when it is collected solely as a replacement of written words. . . .").

49. *Id.* ("The Commission noted that there are important limitations to this policy.").

50. *Id.*

51. *Id.* As will be described later, this exception does not apply to the entirety of children's use of smart speakers, as the purpose of the communication is more than a replacement of written words. Additionally, the audio file will likely contain the child's PII. *See infra* Part III.

the legislation.[52] Because the COPPA requirements are burdensome on the operators, smart speakers were thought to be excluded from the legislation.[53] Yet, smart speakers have been found to fall within COPPA despite the burdensome requirements.[54] And according to the Federal Trade Commission's own guidance, general home devices most likely qualify for the COPPA requirements under "actual knowledge" of having collected children's PII.[55] Given that the latter interpretation is from the Federal Trade Commission (FTC) itself, that is more likely to be the rule that governs with regard to smart speakers since the FTC is the main governing body of COPPA.

COPPA's main focus is on the requirements of the first party operator, but it does mention how third parties play a role in the protection.[56] Based on a law and economics analysis, COPPA, therefore, does not adequately incentivize first parties to comply or first parties to get third parties with whom they share information to comply. And without an incentive to protect the children's information, corporations often "exploit the consumer's behavioral biases."[57] In other words, the regulation is not economically efficient. When the PII that the first party collects will be shared with a third party, the privacy policy must identify that third party, describe what line of business the third party is in, explain how the third party will be using the information, and include whether or not the

52. *See, e.g.*, *Kids & the Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots*, FUTURE OF PRIVACY F. & FAM. ONLINE SAFETY INST. 11 (Dec. 2016), https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf [https://perma.cc/JVB6-ANXY] ("The market for connected smart home devices is growing rapidly, but most general purpose home devices are not – and should not be – covered by COPPA.").

53. *Id.* ("[I]t does not make sense for either operators or all users of a general market device to be burdened with the extra requirements of COPPA because of the possibility that a child might use that device.").

54. *Id.* (using the example of Smarty by Silicone Home, Inc., which is a smart speaker designed to be used by children that would likely be considered "directed to" children and therefore fall within COPPA).

55. *Children's Online Privacy Protection Rule: Not Just for Kids' Sites*, FED. TRADE COMM'N (Apr. 2013), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites [https://perma.cc/MY4Y-U4NG] ("[T]he FTC has said that an operator has actual knowledge of a user's age if the site or service asks for – and receives – information from the user that allows it to determine the person's age.").

56. Ciocchetti, *supra* note 5, at 75–76 (explaining how one of the requirements of COPPA is for the sites' privacy policies to say whether the information will be disseminated to third parties); 15 U.S.C. § 6502(b)(1)(A)(i) (1998).

57. Oren Bar-Gill, *Seduction by Plastic*, 98 NW. U. L. REV. 1373, 1373 (2004).

third party has agreed to maintain the same protections of the PII, including confidentiality, security, and integrity.[58] The FTC said that the first party is largely responsible for making sure that the third party with which they share a child's PII protects the "confidentiality and security" of that information through the contracts between the two parties.[59] The FTC also said that making sure the third party actually does maintain the confidentiality and security of the PII is up to the first party.[60] Additionally, there has to be an element of choice when sharing PII with third parties.[61]

2. 2013 Amendments

In 2013, the FTC amended COPPA.[62] The main effects of the amendments were to: (1) expand the definition of "operator" to include services which integrate third parties that collect a child's PII as part of the first party service; (2) increase the acceptable forms of acquiring parental consent; (3) provide new exceptions to the notice and consent requirements; (4) require more data security protections; and (5) require adoption of reasonable data retention and deletion procedures.[63] Additionally, the amendment expanded the definition of "personal information" to include geolocation information, screen or username, persistent identifiers such as cookies that track a child's activity online, and photos or videos containing the image of a child or audio files containing a child's voice, the focus of this paper.[64] The amendment also changed the definition of "collects" or "collection" to "requesting, prompting, or encouraging a child to submit personal information

58. Ciocchetti, *supra* note 5, at 82 (listing the requirements of the privacy policies).

59. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions [https://perma.cc/YEL9-YEJA].

60. *Id.*

61. 16 C.F.R. § 312.5(a)(2) (2013).

62. *Revised Children's Online Privacy Protection Rule Goes into Effect Today*, FED. TRADE COMM'N (July 1, 2013), https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect [https://perma.cc/3DFL-CPCB] ("The Federal Trade Commission's revised Children's Online Privacy Protection Act Rule took effect today, giving parents greater control over the online collection of their children's personal information.").

63. Phil Nicolosi, *What Will COPPA Changes Mean for Your Business?*, PHIL NICOLOSI L., P.C., https://www.internetlegalattorney.com/coppa-changes-businesses/ [https://perma.cc/XU7E-WAUN] (explaining the changes to COPPA in the new version of the Act).

64. *Revised Children's Online Privacy Protection Rule Goes into Effect Today*, *supra* note 62.

online."[65] The final revision on the definition of "collects" or "collection" results in an implication that becomes central to the argument of this Note: operators cannot evade COPPA by relying on third parties to collect children's PII.[66] Logically, that makes sense since having a third party collect the information is, in essence, no different than direct collection of information by the first party itself.

C. Global Regulatory Framework

This section explores the regulatory backdrop against which COPPA operates. Since many services are used across the globe rather than just within the sphere of one regulation, tech companies must design products for a global marketplace and, as a result, have to follow multiple privacy and data protection laws. Thus, the gaps in COPPA may not be gaps when compared to the entire group of privacy regulations. Similarly, while some of the gaps in COPPA are filled by other regulations, other gaps in COPPA may not currently be filled but should be filled by other regulations as opposed to further amendments to COPPA itself.

1. The General Data Protection Regulation (GDPR)

COPPA is comparable to the General Data Protection Regulation (GDPR), which applies to the European Union, in that both directly address children's privacy online.[67] The GDPR and COPPA fulfill largely the same purpose—children's privacy protections—in two different geographical areas (the European Union and the United States, respectively). The GDPR, though, also covers privacy protections of adults. The GDPR provides lessons with regards to the need for a privacy protection statute with enhanced protections for children. Under the GDPR, online operators are required to obtain parental consent before collecting or using information from children under 16, but member states are allowed to change that age as long as it is not below 13.[68] Furthermore, Articles 13 and 14 of the GDPR state that when a data controller knows that children use its service, the privacy information and communication to

65. Phil Nicolosi, *Can You Avoid COPPA When Third-Parties Collect Data?*, PHIL NICOLOSI L., P.C., https://www.internetlegalattorney.com/avoid-coppa-third-parties-collect-data/ [https://perma.cc/TU2V-UK7G].

66. *Id.*

67. General Data Protection Regulation, 2016 O.J. (L 119) 1.

68. van der Hof, *supra* note 30, at 425 (explaining how the provision allowing for member states to change the age in the definition of "children" was likely a compromise between EU Parliament and Council).

that user should be tailored so that the child can understand their rights and what is happening with their PII.[69] The Amazon Alexa and Google Assistant violate the GDPR's requirements on collecting, using, and storing children's PII in that no privacy notices tailored specifically to children are available, the information about the processing of the child's information by third parties is confusing, and there is a lack of transparency with regard to profiling.[70] Under European data protection law, consent is one of the most important grounds for the processing of personal data to be done in a lawful manner.[71] The GDPR has been found to be insufficient, and, because of the heavy parental involvement in the child's use of the internet, may exacerbate trust issues in that relationship.[72] Overall, the GDPR has seven principles: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.[73] Since the US has no comparable national privacy law, those principles of the GDPR are not reflected in a similar regulation in the US.

2. The California Consumer Privacy Act (CCPA)

Another regulation which acts in tandem with COPPA is the California Consumer Privacy Act (CCPA).[74] The CCPA has a much smaller scope than COPPA, as the CCPA only applies to California. Furthermore, while COPPA focuses solely on children, the CCPA applies to people of all ages, with only certain sections focusing on children in particular. Under the CCPA, a child is defined as any-

69. Anna Morgan, *The Transparency Challenge: Making Children Aware of Their Data Protection Rights and the Risks Online*, 23 J. OF COMPUT., MEDIA & TELECOMMS. L. 44, 46 (2018).

70. Sophie-Charlotte Lemmer, *Alexa, Are You Friends with My Kid? Smart Speakers and Children's Privacy Under the GDPR*, KING'S COLL. LONDON L. SCH. GRADUATE STUDENT RSCH. PAPER NO. 2018/9_6, 13 (June 25, 2020) (violating the requirements of Article 12(1) and 13 in conjunction with Recital 58, guidance of the WP29, and ICO guidance).

71. van der Hof, *supra* note 30, at 420 ("[C]onsent is a fundamental legal instrument for *transforming unlawful conduct into lawful conduct*.").

72. *See, e.g.*, Esther Keymolen & Simone Van der Hof, *Can I Still Trust You, My Dear Doll? A Philosophical and Legal Exploration of Smart Toys and Trust*, 4 J. CYBER POL'Y 143, 154 (2019) ("Giving parents the ability to check their children's conversations with smart toys, potentially even behind their backs, raises new trust issues in their relationship.").

73. *See, e.g.*, Matt Burgess, *What Is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Mar. 24, 2020, 4:30 PM), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 [https://perma.cc/PT49-98X2].

74. California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2018).

one under the age of 16.[75] The CCPA further requires the consent of parents in order for an operator to sell a child's information if that child is under the age of 13.[76] The CCPA requires businesses to disclose what information they have about a user and how they are using or plan to use that information, to delete PII, and not to sell the PII, including to third parties, when a user so requests.[77] Those rights also apply before providing one's PII, or at the time the business is collecting one's PII.[78] The business is not allowed to discriminate against a user for exercising their rights under the CCPA.[79] Similarly, a business cannot require a user to waive their rights under the CCPA, making any contractual provision of such requirement unenforceable.[80] While the CCPA includes many details about what practices are allowed or prohibited in the state, one example of something that is required in California by the CCPA but not required in other states is a "Do Not Sell My Personal Information" home page link.[81] Furthermore, the CCPA covers many more entities, raises the age of "children" from 13 to 16, and expands the definition of "personal information," amongst other changes.[82]

3. The United Nation's Convention on the Rights of the Child (UN-CRC)

Children's online rights have increasingly intersected with children's rights instruments, such as the UN's Convention on the Rights of the Child (UN-CRC).[83] Though the UN-CRC is not a regulation, it provides more context to COPPA and the rationales be-

75. *See, e.g.*, Amelia Vance et al., *Child Privacy Protections Compared: California Consumer Privacy Act v. Proposed Washington Privacy Act*, FUTURE OF PRIV. F. (Jan. 27, 2020), https://fpf.org/2020/01/27/child-privacy-protections-compared-california-consumer-privacy-act-v-proposed-washington-privacy-act/ [https://perma.cc/58FU-JEZ4].

76. *See id.*

77. *Cal. Consumer Priv. Act (CCPA)*, STATE OF CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa [https://perma.cc/MYN5-YYLM].

78. *Id.*

79. *Id.*

80. *Id.*

81. *See, e.g.*, Spencer Persson et al., *California Passes Major Legislation, Expanding Consumer Privacy Rights and Legal Exposure for US and Global Companies*, DATA PROTECTION REPORT (June 29, 2018), https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/ [https://perma.cc/9FYB-F9E7].

82. *See id.*

83. *See, e.g.*, Sonia Livingstone, *Reframing Media Effects in Terms of Children's Rights in the Digital Age*, 10 J. OF CHILD. & MEDIA 4, 5 (2016) (explaining how the coincidence of the 25th anniversary of the UN-CRC and the 25th anniversary of the World Wide Web being in the same year led to researchers and policymakers

hind it. Many ideas and values discussed at the UN-CRC are incorporated into statutes and regulations such as the GDPR, CCPA, and COPPA. The UN-CRC describes the "3Ps" every child has as the rights to the provision of basic needs, protection against neglect, and participation in families and communities.[84] Those "3Ps" are helpful in navigating children's rights not only offline, but online as well.[85]

D. How the FTC Has Dealt with Enforcement

The FTC has primary enforcement authority of COPPA. The harm from COPPA violations falls directly on the children who are the users of the service through the release of their PII. The FTC's first enforcement action was against Toysmart.com on July 10, 2000 to block it from selling confidential information about its consumers.[86] About a month before the suit was filed, the company filed for bankruptcy.[87] In doing so, Toysmart.com purchased a newspaper advertisement announcing the sale of its assets, including its customer information, despite promising customers that information would never be shared.[88] The FTC also found that Toysmart.com collected PII of children under 13 including names, email addresses, and ages without notifying parents or obtaining parental consent.[89]

As of 2019, the FTC had brought close to 30 COPPA cases and had collected hundreds of millions of dollars in civil penalties.[90] Some of those actions included suits brought by the FTC against

looking into the "connections between internet governance and children's well-being").

84. *See id.*

85. *See* Sonia Livingstone & Brian O'Neill, *Children's Rights Online: Challenges, Dilemmas, and Emerging Directions*, MINDING MINORS WANDERING THE WEB 19, 19 (Simone van der Hof et al. eds., Mar. 2014) ("[T]he UN Convention on the Rights of the Child is helpful in mapping children's rights to provision, protection and participation as they apply online as well as offline.").

86. *See* Stephanie Stoughton, *FTC Seeks to Stop Waltham, Mass.-Based e-Retailer from Selling Consumer Data*, BOS. GLOBE (July 11, 2000).

87. *See id.*

88. *See FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, FED. TRADE COMM'N (July 21, 2000), https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding [https://perma.cc/JW2U-YPR6].

89. FTC v. Toysmart.com, No. 00-CV-11341-RGS, 2000 U.S. Dist. LEXIS 21963, at *1 (D. Mass. Aug. 21, 2000).

90. F.T.C., PRIVACY & DATA SECURITY UPDATE: 2019 (2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf [https://perma.cc/Q8CC-HS3H].

Vtech,[91] Hello Barbie,[92] Google and YouTube,[93] TikTok,[94] and HyperBeard.[95] In 2015, Vtech announced that 5 million users' data, including that of children, was compromised as part of a cyberattack.[96] The data compromised was sufficient to link children back to their family's last name and home address.[97] The settlement with Google and its subsidiary, YouTube, required YouTube to "modify its technology platform to allow greater monitoring of third parties' COPPA compliance - beyond that required by law."[98] On February 27, 2019, the FTC obtained a settlement from TikTok for $5.7 million, the largest COPPA penalty so far, over allegations that the company collected personal information from children without parental consent as required by COPPA.[99] Finally, on June 4, 2020, HyperBeard, Inc. agreed to settle for $150,000 and to delete the PII it had illegally collected from children.[100] HyperBeard, Inc. also allegedly violated COPPA by allowing third parties to collect persistent identifiers, included in the definition of PII as of the 2013

91. *See* Andrea Peterson, *Toymakers Are Tracking More Data About Kids – Leaving Them Exposed to Hackers*, WASH. POST (Nov. 30, 2015, 12:40 PM), https://www.washingtonpost.com/news/the-switch/wp/2015/11/30/toymakers-are-tracking-more-data-about-kids-leaving-them-exposed-to-hackers/ [https://perma.cc/UQZ8-XF9Y] (detailing the hacking of Vtech).

92. *See* Donnell Holloway & Lelia Green, *The Internet of Toys*, COMMC'N RSCH. AND PRAC. (2016).

93. *See* PRIVACY & DATA SECURITY UPDATE: 2019, *supra* note 90, at 9 ("The FTC's settlement with Google and its subsidiary YouTube – brought in conjunction with the New York Attorney General – alleges that the company collected kids' personal data without parental consent, in violation of the COPPA Rule.").

94. *See Children's Online Privacy Protection Act*, *supra* note 8.

95. *See Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data Without Parental Consent*, FED. TRADE COMM'N (June 4, 2020), https://www.ftc.gov/news-events/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it [https://perma.cc/5PQS-HF9B] ("In a complaint filed by the Department of Justice on behalf of the FTC, the Commission alleges that HyperBeard, Inc. violated the Children's Online Privacy Protection Act Rule (COPPA Rule) by allowing third-party ad networks to collect personal information in the form of persistent identifiers to track users of the company's child-directed apps, without notifying parents or obtaining verifiable parental consent.").

96. Peterson, *supra* note 91.

97. *Id.*

98. Duane C. Pozza, *FTC Pushing to Hold Companies Liable for Third Parties' Activities*, WILEY CONNECT (Oct. 21, 2019), https://www.wiley.law/newsletter-2019-Oct-PIF_FTC_Pushing_to_Hold_Companies_Liable_for_Third_Parties_Activities [https://perma.cc/7MAA-LMTB].

99. *Children's Online Privacy Protection Act*, *supra* note 8.

100. *Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data Without Parental Consent*, *supra* note 95.

amendments, which allowed the company to track the users of apps, including apps directed at children, without notifying parents or obtaining parental consent.[101] The settlement amounts in the above lawsuits are very small compared to the size and net worth of the firms.[102] The real harm to the companies comes from the reputational damage of being seen as a dangerous service for children to use. Compliance with COPPA would not only help firms avoid minor monetary damages but also frame them as willing to do what is necessary to keep children safe.

III.
AMAZON ALEXA AND GOOGLE ASSISTANT

In order for the FTC to enforce the regulation, they first have to identify companies that are not in compliance. The first place to look to determine whether Amazon Alexa and Google Assistant comply with COPPA is their own privacy policies, to see whether the first parties themselves facially comply. For products made by companies as large as Google and Amazon, looking at their privacy policies is not as easy as following one link to a single document with all the information one is looking for. Rather, finding a specific piece of information requires searching through multiple different privacy policies, each privacy policy tailored to a particular type of user or product.[103]

Smart speakers and devices pose especially great dangers to children in terms of collecting, storing, using, and sharing children's PII because of the nature of the interactions with these devices. The speakers encourage the user to disclose large amounts of personal data about their lives, and since children are not as critical as adults in disclosing such information, the devices pose an even greater danger.[104] Children might also not understand the extent

101. *Id.*

102. *See, e.g.*, Sam Shead, *TikTok Owner Bytedance Reportedly Made a Profit of $3 Billion on $17 Billion of Revenue Last Year*, CNBC (May 27, 2020, 9:08 AM), https://www.cnbc.com/2020/05/27/tiktok-bytedance-profit.html [https://perma.cc/GN76-LQA4] (stating that TikTok's revenue in 2019 was $17 billion).

103. Yet, as will be shown, some of the privacy policies contradict each other, leaving a user confused and lacking in knowledge as to what information is being collected, used, and disclosed, and for what purposes.

104. *See Internet Safety for Kids: How to Protect Your Child from the Top 7 Dangers They Face Online*, KASPERSKY, https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online [https://perma.cc/8UF8-CG3B] (last visited Mar. 22, 2022) ("Children do not yet understand social boundaries. They may post personally identifiable information (PII) online, for example in their social media profiles, that should not be out in public.").

to which their voices and conversations can be recorded through a device which has no screen and requires no physical interaction to use.[105] The lack of screen and lack of physical interaction to use the Amazon Alexa and Google Home also provide greater obstacles for complying with COPPA, as there is not as easy of a way to require parental consent or verification before the child begins using the device. There is also the problem of recognizing when a child is using the smart speaker as opposed to an adult.[106] Another challenge is that the device can be accessed accidentally, simply by speaking aloud and the speaker hearing what was said, rather than something like an app which is intentionally opened or setting up an account and clicking "I agree" to access a service.[107]

Both Amazon and Google neglect to address what is referred to as "The Playdate Problem."[108] Regardless of whether Amazon and Google set up separate children's accounts or protect the children of the family in some other way, they do not describe how they obtain parental consent from the parent or guardian of a child using the service who does not live with the owner of the device. The failure to obtain parental consent, in itself, is a violation of COPPA that the privacy policies and notices do not mention. Similarly, the smart speakers do not distinguish between a child's voice and an adult's voice, opening up a search to include potentially inappropriate responses when a child is interacting with the device.

---

105. *See, e.g.*, *The Dangers of Smart Speakers and Essential Safety Tips*, NEXUS (Aug. 7, 2019), https://nexusconsultancy.co.uk/blog/the-dangers-of-smart-speakers-and-essential-safety-tips/ ("In order to be useful to their owners, smart speakers and other connected devices are always listening.").

106. *See* Martyn Farrows, *Let's Talk Voice Tech, Data Privacy, and Kids*, VOICEBOT.AI (Mar. 28, 2020, 1:00 PM), https://voicebot.ai/2020/03/28/lets-talk-voice-tech-data-privacy-and-kids/ [https://perma.cc/JL3G-4WFT] ("Once consent was given, a kid's data was treated just like the data of an adult.").

107. *See, e.g.*, Tove Marks, *The Privacy Risks of Your Smart Speaker*, VPNOVERVIEW (Dec. 18, 2020), https://vpnoverview.com/privacy/devices/privacy-risks-smart-speaker/ [https://perma.cc/Q7P4-GT2U] ("Your smart speaker may think it heard the keyword but simply misinterpreted a snippet of conversation. This can have the smart speaker listening for your instructions and possibly taking actions based on what it thinks it hears.").

108. *See*, *e.g.*, *Echo Dot Kids Edition Violates COPPA*, ECHO KIDS PRIV., https://www.echokidsprivacy.com/ [https://perma.cc/UW9T-7GXL] (last visited Jan. 11, 2022) (defining the Playdate Problem as Amazon not giving notice or obtaining parental consent "before recording the voices of children that do not live in the home (visiting friends, family, etc.) with the owner of the device. They advertise having the technology to create voice profiles for customized user experiences but fail to use it to stop information collection from unrecognized children.").

A. How Smart Speakers Operate

Before looking into the specifics of the privacy policies, it is essential to understand how the smart speakers work. The speaker is triggered to activate when it hears its "wake word."[109] The device then records the communication and sends it to a Cloud where the communication is transcribed to text and analyzed with natural language processing before sending back to the smart speaker the information to complete the request or task.[110] In terms of terminology, the Google Home and Google Nest are the hardware connected to Google Assistant, the software, and the Amazon Echo is the hardware supported by Amazon Alexa, the software.[111]

B. Amazon Alexa

On its face, Amazon complies with COPPA. Yet, when looking into the details of their policies, one can see how they do not comply with the requirements in ways that an average consumer might not understand. The general Amazon privacy policy states, "[w]e do not knowingly collect personal information from children under the age of 13 without the consent of the child's parent or guardian. For more information, please see our Children's Privacy Disclosure."[112] Following the provided link leads to the Children's Privacy Disclosure, which specifies that some of Amazon's services are directed to children and that Amazon has "actual knowledge" that some of its services are used by children.[113] That recognition is important because it signifies that Amazon must be in compliance with COPPA.[114] Amazon follows that recognition by saying, "[i]n these situations, children may share and we may collect personal information that requires verifiable parental consent under the Children's Online Privacy Protection Act."[115] According to those statements, one would reasonably believe that Amazon is in compliance, as they even go so far as to name the specific Act they are

109. *See* Matthew B. Hoy, *Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants*, 37 MED. REFERENCE SERVS. Q. 81, 82 (2018) ("The software constantly listens for a key word to wake it up.").

110. *Id.*

111. Lemmer, *supra* note 70, at 2.

112. *Amazon.com Privacy Notice*, AMAZON (last updated June 29, 2022), https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 [https://perma.cc/J9R9-WP5V].

113. *See Children's Privacy Disclosure*, AMAZON (last updated July 8, 2020), https://www.amazon.com/gp/help/customer/display.html?nodeId=202185560 [https://perma.cc/8NDD-UHKZ].

114. *See supra* Part II(B).

115. *Children's Privacy Disclosure*, *supra* note 113.

subject to. Amazon continues in describing the use of the PII they collect from children: "to provide and improve our products and services, including personalizing offerings and recommendations for children, communicating information, enforcing parental controls, and giving parents visibility into how their children use our products and services."[116]

The Children's Privacy Disclosure continues with more of what appears to be compliance with COPPA. The Disclosure states:

> You choose whether to give us permission to collect Child Personal Information from your child. If you have not given us permission to collect Child Personal Information, we may make available certain voice services intended for children (e.g., certain Alexa features), and we may process your child's voice recordings to provide these services, but we will not store those voice recordings. We do not knowingly collect, use, or disclose Child Personal Information without this permission.[117]

This information is contradictory and misleading. Processing a child's information may be sufficient for the PII to then be disclosed to third parties.[118] And, as explicitly stated in the notice, "[t]his disclosure does not apply to the practices of any third-party services (including apps, skills, and websites) that may be accessed through an Amazon product or service."[119] So any information that is shared or transferred from Amazon to a third party is not necessarily protected in the same, if any, way at all.

The first issue in Amazon's compliance arises when they try to distinguish Amazon's sharing of a child's PII with the child sharing their own PII: "[y]our child may be able to share information publicly and with others depending on the products and services used."[120] Despite Amazon's attempt to distinguish the ways in which information is shared to protect themselves from liability, COPPA covers all information collected by a service from a child regardless of whether the child or the company is the one sharing the information. Though this speaks to breach of regulation directly in the privacy policy rather than breach of regulation due to a lack of a requirement in the privacy policy, it demonstrates that Amazon does not comply, even facially.

A complaint to the FTC on May 9, 2019 regarding the Echo Dot Kids Edition, a smart speaker specifically targeted for children,

116. *Id.*
117. *Id.*
118. *See infra* Part IV.
119. *Children's Privacy Disclosure*, *supra* note 113.
120. *Id.*

illustrates the ways in which Amazon does not comply with COPPA, even on its face.[121] The Echo Dot comes with a one-year subscription to Amazon's FreeTime Unlimited, a service that provides access to entertainment including books, music, and "Kid Skills."[122] The complaint alleges that the product is subject to COPPA, yet the notice to parents and online Children's Privacy Disclosure are lacking in satisfying the requirements of COPPA.[123] In addition to making claims that the privacy policies are confusing and contradictory, the complaint argues that the system for obtaining consent is inadequate because it does not verify that the person consenting is actually the parent, or even an adult at all.[124] Furthermore, Amazon keeps the audio recordings until they are deleted by a parent, which is in violation of the COPPA requirement that the information be stored only as long as necessary. Even when a parent tries to delete the audio recordings, the voice transcriptions of those audio recordings are still saved.[125] Furthermore, deleting recordings is burdensome on the parent who would have to open the Alexa app on their phone, go to "Settings," select "History," and then listen to each individual recording to figure out which ones they want to be deleted.[126] While the complaint concerns the Echo Dot Kids Edition, the deficiencies in compliance with COPPA apply in the same way to Amazon Alexa more generally, especially since the main difference between the Echo Dot Kids Edition and the Echo Dot is that the Echo Dot Kids Edition includes a one-year subscription to Amazon's FreeTime Unlimited service and a two-year warranty that covers intentional damage to the device caused by a child.[127]

121. Complaint at 25, 30, *In re* Request for Investigation of Amazon, Inc.'s Echo Dot Kids Edition for Violating the Children's Online Privacy Protection Act (F.T.C. May 9, 2019) [hereinafter Amazon Complaint] (listing some of the failures of compliance, such as the burdensome nature of reviewing information, not checking that the parental consent is from a parent of the child, storing the child's PII forever, and more).

122. *Id.* at iii.

123. *Id.* at iv ("Neither [Amazon's direct notice to parents nor its online Children's Privacy Disclosure] provides parents with the information they need to make an informed decision about whether to give consent.").

124. *Id.* at v ("[Amazon's system] does not verify that the person 'consenting' is the child's parent as required by COPPA. Nor does Amazon verify that the person consenting is even an adult because it allows the use of debit gift card and does not require a financial transaction for verification.").

125. *Id.* ("[U]nless a parent deletes the recording of a child's voice, Amazon will retain those recordings indefinitely.").

126. Candid Wueest, *A Guide to the Security of Voice-Activated Smart Speakers*, SYMANTEC 18 (Nov. 2017), https://docs.broadcom.com/doc/istr-security-voice-activated-smart-speakers-en [https://perma.cc/AE3G-CZ7X].

127. Amazon Complaint, *supra* note 121, at 4.

C. Google Assistant

Mirroring the confusing and contradictory nature of Amazon's many privacy policies and notices regarding the collection, storage, use, and sharing of children's PII, Google has multiple documents describing the privacy of one's information. The Google Nest has its own privacy policy, which, contrasting Amazon's acknowledgement that they collect information from children, states that "[o]ur Site does not knowingly collect or store any personal information about children under the age of 13."[128] That statement implies that COPPA does not apply at all, so there are no enhanced protections for children's information. Yet denying that a service is used by anyone under the age of 13 is exactly what has been argued that Facebook should be found liable for, in violation of COPPA due to the "actual knowledge" that children were using the product and service.[129] The incorporation of children's features into Google Home and Google Nest, as well as the encouragement of placing the device in a "family room" is sufficient for Google to have "actual knowledge" that a child under the age of 13 would be using the service, so their information and communications would be collected and stored.[130]

Searching through the Google Privacy & Terms site and navigating through multiple links, Google provides a privacy notice that directly applies to the collection of voice and audio information from "Children's Features" on Google Assistant.[131] If one is able to find that particular privacy notice, one would know that Google's main privacy policy does not state all of the privacy terms: "[i]n addition to the information provided in the Google Privacy Policy

128. *Privacy Policy for Nest Web Sites*, NEST (Jan. 31, 2020), https://nest.com/legal/privacy-policy-for-nest-web-sites/ [https://perma.cc/7ZK8-768K].

129. *See* Shannon Finnegan, *How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future*, 50 SETON HALL L. REV. 827, 828 (2020) ("Since COPPA's enactment in 1998, Instagram and Facebook (collectively 'Facebook, Inc.') have effectively managed to circumvent the requirements imposed on websites under COPPA by simply banning users under the age of thirteen from their websites. This restriction does not adequately prevent children from accessing these websites.").

130. GOOGLE NEST MINI, (last visited Jan. 12. 2022), https://store.google.com/us/product/google_nest_mini?hl=EN-US [https://perma.cc/5UZX-S5CV].

131. *Privacy Notice for Voice and Audio Collection from Children's Features on Google Assistant*, HEY GOOGLE (Aug. 5, 2020), https://assistant.google.com/privacy-notice-childrens-features/ [https://perma.cc/A6D8-9266] (signaling that the privacy notice applies to collection of children's data through smart speakers in the title of the privacy notice, "Privacy Notice for Audio Collection from Children's Features on Google Assistant").

this Privacy Notice also applies to the use of these features on Google Assistant."[132] That notice directly violates COPPA, stating, "[i]f you interact with children's features-like Assistant for Families Actions or YouTube Kids videos-on Google Assistant, we briefly collect voice and audio recordings of those interactions. This information is processed to allow for use of the audio feature, so we can fulfill the interaction, and immediately deleted."[133] While the immediate deletion may appear sufficient, the violation comes from the fact that there is no parental consent obtained before collecting the child's information. Regardless of how long the information is stored for, parental consent is required for any information to be collected at all.[134] While Google may argue that its process falls under § 6502(b)(2)(A), where parental consent is not required, Google's privacy policy does not state that it applies only to online contact information.[135]

Google also has a privacy notice for Google accounts managed with Family Link, specifically for children under 13.[136] As with the previous notice, this one was also difficult to find, not being readily apparent, yet it controls over the main privacy notice: "[t]o the extent there are privacy practices specific to your child's account or profile, such as with respect to limitations on personalized advertising, those differences are outlined in this Privacy Notice."[137] Not only is Google recognizing that there are contradictory terms in the privacy policies, but it is also stating that the somewhat hidden notice is the one that controls. Just like Amazon, the notice states, "[t]his Privacy Notice does not apply to the practices of any third party (non-Google) apps, actions or websites that your child may use."[138] As a result, any information shared with third parties is under different protections, if it is under any protections at all.

---

132. *Id.*

133. *Id.*

134. 15 U.S.C. § 6502(b)(1)(A)(ii) (1998).

135. 15 U.S.C. § 6502(b)(2)(A) (1998); *Google Privacy Policy*, GOOGLE, https://policies.google.com/privacy?hl=EN-US [https://perma.cc/9PDF-52MU] (last visited Aug. 8, 2022).

136. *Privacy Notice for Google Accounts Managed with Family Link, for Children Under 13*, GOOGLE, https://families.google.com/familylink/privacy/child-policy/ [https://perma.cc/E23W-XQS3] (last visited Aug. 8, 2022) (signaling that the privacy notice applies to children under 13 in the title of the privacy notice, "Privacy Notice for Google Accounts and Profiles Managed with Family Link, for Children under 13 (or applicable age in your country)").

137. *Id.*

138. *Id.*

The children's policy is in direct violation of COPPA for storing voice and audio information from children under the age of 13 without any mention of many of the requirements in COPPA: "[w]e automatically collect and store certain information about the services your child uses and how your child uses them. . . ."[139] Among the various information collected is the child's activity, location information, and voice and audio information, which falls within the category of PII, covered by COPPA.[140] Google does describe the uses of the information collected as to "provide, maintain, and improve our services; to develop new services; to customize our services for your child; to measure performance and understand how our services are used; to communicate directly with your child in relation to our services; and to help improve the safety and reliability of our services,"[141] but it does not require parental consent, one of the main requirements of COPPA.

Google's policy also demonstrates the problems of data sharing across different companies. The policy states, "we may combine the information we collect among our services and across your child's devices for the purposes described above. Depending on your child's account or profile settings, their activity on other sites and apps may be associated with their personal information in order to improve Google's services."[142] Not only is Google aggregating a child's PII, creating a database of their information, but it is combining the information it directly collects about a child with information it gathers from other sources, increasing the size of the child's database of PII and increasing the risks and dangers of that child due to the exposure of their information.

Overall, the Google Assistant does not comply with COPPA, even on its face. Beyond the contradictions and direct violations mentioned previously, Google Assistant allows a parent to set up an account for a child, but if the parent chooses not to, or if the child uses the device when not linked to their own account, the Google Assistant collects, uses, stores, and shares the information in the same way it does for adults, despite the COPPA requirements.[143]

---

139. *Id.*

140. *Id.* (listing information the service collects: "Information you and your child create or provide to us; Information we get from your child's use of our services [which includes] Your child's apps, browsers & devices, Your child's activity, your child's location information, [and] your child's voice & audio information").

141. *Id.*

142. *Id.*

143. Lemmer, *supra* note 70, at 5 ("If the kid's Google Account is not linked to the device, it will operate for it like for adults.").

The process for deleting specific recordings is taxing on the parent due to the necessity of searching through all of the individual recordings to find the ones that the parent would like to delete, just as that of Amazon.[144] For Google, the list of recordings includes not only audio files but search history, among other data, making the list of files the parent must look through even longer.[145]

IV.
INSUFFICIENCY OF FIRST PARTY COMPLIANCE

Direct compliance with COPPA, contrasted with compliance with the spirit of the law, would still be insufficient when it comes to protecting children's information because of the increased role of third-party data collection and sharing.

A. Overview of the Role of Third Parties

Most of the Kid Skills on the Amazon Alexa and the Family Actions on the Google Assistant are provided by third parties.[146] When children use those apps, Amazon and Google collect voice data that is sent to the third party; this data may be the audio file itself or a transcription of the communication.[147] Whether or not the third parties actually process the data is irrelevant in the safety and protection of children's PII and in complying with COPPA.[148]

Furthermore, the processing and use of the children's data by third parties should be readily available information to a parent in the first party's privacy policy rather than the parent having to identify when their child leaves the first party to go to a third-party app, locating the privacy policy of that third party, and figuring out whether the third party is in compliance with COPPA and protects their child's information to the degree desired. The Statement of Basis and Purpose of COPPA highlights how "it cannot be the responsibility of parents to try to pierce the complex infrastructure of

144. Wueest, *supra* note 126, at 18 (explaining the process for deleting recordings).

145. *Id.*

146. Lemmer, *supra* note 70, at 12 ("[Kid Skills or Family Actions] are mostly provided by third parties and not directly by Amazon or Google.").

147. *Id.* ("Amazon and Google collect the voice data during the use of the skill, and send the transcripts to the third party to enable them to deliver their service.").

148. *Id.* at 13 ("Amazon and Google must address children with tailored privacy notices before their data are processed during their use of kid features. However, Amazon and Google decide not to provide children at all with information about their privacy.").

entities that may be collecting their children's personal information through any one site."[149] The Act continues, "[f]or child-directed properties, one entity, at least, must be strictly responsible for providing parents notice and obtaining consent when personal information is collected through that site. The Commission believes that the primary-content site or service is in the best position to know which plug-ins it integrates into its site, and is also in the best position to give notice and obtain consent from parents."[150]

According to that recommendation by the Commission, Amazon and Google should be held responsible not only for their own compliance with COPPA, but also for notifying parents of compliance of third parties that a child might access through the first party. Home devices, as they relate to third parties within the regulations of COPPA, are very similar to any other service that is regulated by COPPA. This Note looks at smart speakers and devices in particular because of the difficulties they present in complying with COPPA, which are then exacerbated by third-party sharing, creating a system in which greater information is at risk than with devices other than smart speakers which do not face the same initial challenges with compliance. To summarize, smart speakers and third-party sharing release much greater quantities, in much greater quality, of information and specifically of children's information.

B. Amazon

Kid Skills are apps run by their own privacy policies but accessed through the Alexa device.[151] Amazon represents that these skills are safe for children.[152] In setting up the FreeTime Unlimited account—through which the Kid Skills are accessed on the Alexa—a parent can add a child's profile and will be prompted to give "permission to collect personal information including voice recordings."[153] The notice states that the "permission will apply to all Alexa devices, skills, and other Amazon kid services."[154] Not only is

149. Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3977 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312).

150. *Id.*

151. Kid Skills are a feature of the Amazon Alexa directed at children. *See supra* Part III(B); *see also* Amazon Complaint, s*upra* note 121, at iv ("Amazon states that its Children's Privacy Disclosure does not apply to third-party services, including skills, and that before using a third-party service, parents should review the skill's policies concerning data collection and use.").

152. Amazon Complaint, *supra* note 121, at 7.

153. *Id.* at 8 (internal quotation marks omitted).

154. *Id.* (internal quotation marks omitted).

that statement vague as to whether the Kid Skills, which are on third-party apps, are included in "other Amazon kid services," but it directly contradicts an earlier rule that Amazon has for Kid Skills in which they cannot collect PII.[155] To finish setting up a child's FreeTime Unlimited profile, someone has to enter the Amazon password and verify that they are an adult by providing the security code for a credit card.[156] Disposable gift cards are acceptable in verifying that one is an adult with a security code.[157] Ultimately, the parent is asked to agree to "Parental Consent."[158]

Third parties play a larger role in the Amazon Alexa realm than just with Kid Skills. The emphasis on Kid Skills shows the direct need for COPPA compliance because the services are targeted at children, but the use of the Amazon Alexa device in the broader home by children is enough to require compliance with the regulation through "actual knowledge." Amazon mentions the collection and sharing of PII from interacting with Alexa to third parties in its privacy notice: "[w]e employ other companies and individuals to perform functions on our behalf. . . . These third-party service providers have access to personal information needed to perform their functions, but may not use it for other purposes."[159] By sharing PII, whether it be that of an adult or child, with third parties, Amazon is releasing that information out to other companies who, as stated in Amazon's privacy notice, do not follow the same privacy protection measures that Amazon does. This leads to a domino effect where one third party may then share the PII with others, increasing the spread and transmission of the data. Due to the enhanced risks and threats of the disclosure and spread of children's PII, as mentioned earlier,[160] this domino effect is especially problematic for children whose information is supposed to be given heightened protection under COPPA.

Amazon's disclaimer about the practices of third parties, including those of Kid Skills which are directly targeted to children, does not satisfy the COPPA requirements. The privacy notice implies that some third parties will collect children's PII, but the no-

155. *Id.*

156. *Id.* at 9.

157. *Id.* ("This interface accepts any type of payment card, including disposable gift debit cards which are frequently given to children.").

158. *Id.* I will not dwell on the issue here, as it again is not the focus of this Note, but it is important to highlight that Amazon itself is not in compliance with COPPA by allowing for a parental consent and verification process that is easily satisfied by a child, thereby avoiding parental knowledge or consent at all.

159. *Amazon.com Privacy Notice*, *supra* note 112.

160. *See supra* Part I(B).

tice does not list which ones will, nor does it list the types of PII collected or their uses.[161] As of June 25, 2020, 84.6% of Kid Skills did not provide a third-party privacy notice, so there was no way for a parent to know whether or not their child's information was being collected, stored, used, or disclosed with even more companies.[162] For example, LEGO Duplo stories, one of Amazon's offered Kid Skills, provides a link to a generic privacy policy, not specifically related to the Kid Skills, Amazon, or Alexa.[163] The example of LEGO Duplo stories also highlights the contradictory nature of third-parties' privacy policies with first-parties'; while Amazon's developer guidelines state that PII will not be collected, the LEGO privacy policy says that it collects personal data.[164] Those Kid Skills that did include a link led to a general privacy policy without any information on the Amazon Alexa or the Kid Skill in particular.[165] Furthermore, Amazon fails to give notice and obtain parental consent for information that the third parties collect.[166] The 2013 COPPA amendment clarified that the operator of an online service that is directed to children is responsible for not only disclosing and obtaining parental consent for its own collection of children's PII but also for disclosing and obtaining parental consent for the information that third parties collect through the online service.[167]

C. Google

Comparable to Amazon's Kid Skills, Google offers "Family Actions," which are also directly targeted at children. Family Actions provide content specifically for children which is mostly provided

161. *Echo Dot Kids Edition Violates COPPA*, *supra* note 108 ("Amazon does not disclose which kid skills (developed by 3rd parties) collect child personal information or what they collect. It tells parents to read the privacy policy of each kid skill (impermissible under COPPA).").

162. Lemmer, *supra* note 70, at 14.

163. *Id.* at 15.

164. *Id.*

165. *See* Amazon Complaint, *supra* note 121, at 24–25 ("We also examined several of those privacy policies, and found that they typically link to the developer's general children's privacy policies, which generally contain lots of extraneous information and provide no specific information about the data collected using the Echo Dot Kids Edition.").

166. *See id.*

167. *See Amended COPPA Rule Comes into Effect*, PRIV. & INFO. SEC. L. BLOG (July 1, 2013), https://www.huntonprivacyblog.com/2013/07/01/amended-coppa-rule-comes-into-effect/ [https://perma.cc/RD33-6Y5B] ("The revised Rule requires apps and websites directed at children to give parental notice and obtain consent before permitting third parties to collect children's personal information through plug-ins.").

by third parties.[168] A child can open the Family Actions with a voice command where no parental consent is obtained, and no privacy warning or notice is provided.[169] This is directly in violation with COPPA. Yet, the direct violation is not the only way in which Google fails to comply with the regulation. Just like Amazon, Google is responsible for the protection of children's information once that information is transferred or shared to third parties. Google's Privacy Notice for Google Accounts Managed with Family Link for Children Under 13 states, "[i]nformation we collect may be shared outside of Google in limited circumstances. We do not share personal information with companies, organizations, and individuals outside of Google except in the following cases[.]"[170] The notice goes on to list when PII will be shared with consent, with your family group, for external processing, and for legal reasons.[171] The inclusion of "with consent" as its own category suggests that the times children's PII is shared through the other listed categories do not require parental consent, as required by COPPA.

In the same way as Kid Skills, only some Family Actions provide links to privacy policies.[172] Those that do link to their general privacy notice, not anything particular to the Family Action, Google, or Google Assistant.[173] For example, Disney's "Wreck it Ralph Adventure," a Family Action through Google Assistant, provides a link to its Privacy Policy, but that link brings you to the company's general privacy policy.[174] Even when third parties include a privacy policy, regardless of whether or not it is particular to Family Actions or just the company's general privacy policy, that link is difficult to locate through Google Assistant.[175] In order for a parent to find the privacy policy, they would have to actively seek it out on the Google Assistant's webpage rather than being provided with it when opening the Family Action.[176]

Many studies and much research has been done on COPPA as it relates to first parties, but if those first parties are sharing the children's personal information with third parties who do not follow the principles or requirements outlined in COPPA, the infor-

168. Lemmer, *supra* note 70, at 5.
169. *Id.* at 19.
170. *Privacy Notice for Google Accounts Managed with Family Link, for Children Under 13*, *supra* note 136.
171. *Id.*
172. Lemmer, *supra* note 70, at 15.
173. *Id.*
174. *Id.* at 46.
175. *Id.* at 14.
176. *Id.*

mation is essentially just as available and unprotected as if COPPA did not exist at all. The third parties that receive the children's PII could then share with others creating the domino effect described above. The increased sharing of information to third parties and integration of third-party services into first parties leads to a questioning of the effectiveness of COPPA in protecting children's PII.

V.
SUGGESTIONS

The issue is not only in the statutory language and design but also in the FTC's enforcement. Given the overall lack of compliance, COPPA fails at its goal of protecting children's PII. The Global Privacy Enforcement Network Privacy Sweep of 2015 found that while 67% of websites and apps collected children's PII, only 22% tailored their data protection communications to children in compliance with COPPA.[177] While 59% of apps for kids were found to share personal information, only 11% told the user so.[178] Furthermore, as of 2015, 45% of the 364 kids' apps in Google Play or the Apple App Store had privacy policies that could be accessed through a direct link from the app store page.[179] All of these examples demonstrate how the current regulations are not doing enough to protect children's information to the fullest extent. Not only could the FTC file suit against companies for violating COPPA, but they could also treat those violations as unfair or deceptive acts under the Federal Trade Commission Act.[180] Yet, even if there were compliance, given the current state of data collection and devices such as Amazon Alexa and Google Assistant, COPPA is not sufficient in protecting children's information. The trends of datafication, hyperconnectivity, and commercialization have decreased COPPA's value.[181] COPPA is also no longer relevant given that peo-

177. Morgan, *supra* note 69, at 45.

178. Jim Kreidler, *Are the Apps Your Children Use Illegally Marketing to Them?*, FED. TRADE COMM'N (June 4, 2020), https://www.consumer.ftc.gov/blog/2020/06/are-apps-your-children-use-illegally-marketing-them [https://perma.cc/2G9Q-KYP9].

179. Kristin Cohen & Christina Yeung, *Kids' Apps Disclosures Revisited*, FED. TRADE COMM'N (Sept. 3, 2015, 11:04 AM), https://imperialvalleynews.com/index.php/news/national-news/5104-kids-apps-disclosures-revisited.html [https://perma.cc/JL2M-WENF].

180. Ciocchetti, *supra* note 5, at 77 ("Concerning enforcement, violations of COPPA may be treated as unfair or deceptive acts and/or practices prohibited under the Federal Trade Commission Act (FTC Act) and enforced by the FTC.").

181. Datafication is the trend in which aspects of our lives are turned into a data format. Hyperconnectivity describes the way in which people are constantly

ple do not read privacy policies regardless of how accessible they are.[182] And even when people do read them, they do not understand what is being said.[183] Furthermore, COPPA has become increasingly irrelevant since parents will help their children lie.[184]

With a law and economics perspective in mind,[185] first parties should be held responsible for the ways in which third parties use the information shared with them, regardless of whether or not they are actually being held responsible for that by the FTC. Based on economic efficiency, the first party is in the best position to monitor the third party's compliance without having to establish an entirely separate agency charged with doing so, thereby efficiently allocating resources to where they need to be. Otherwise, the first party's efforts to comply and protect children's information would be meaningless given the expansive use and necessity of third parties, as is evidenced in the Amazon Alexa and Google Assistant. Similarly, under the cheapest cost avoider theory, the first party is best suited to be responsible for the third party since they have the knowledge of which third parties they are going to share with. Arguably, parents should have some of the burden of protecting their children from third parties, as exemplified by the requirements placed on parents through COPPA, but, given that not all first parties disclose who they share information with, the transaction costs of parents holding that responsibility would be great and could be

connected to social networks and sources of information through multiple means of communication. Commercialization is the practice by which something is run mainly for financial gain. *See* van der Hof, *supra* note 30, at 412–18.

182. *See* Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts"*, 78 U. CHI. L. REV. 165, 182 (2011) ("The general conclusion is clear: no matter how prominently EULAs are disclosed, they are almost always ignored."); *see also* Florencia Marotta-Wurgler, *Does Disclosure Matter?* 1 (NYU Ctr. for L., Econ. and Org., Working Paper No. 10-54, 2010) (following the clickstream of 47,399 households to 81 internet software retailers to see whether disclosure leads to more people reading contracts and finding that "making contracts more prominently available does not increase readership in any significant way").

183. *See* Omri Ben-Shahar & Carl Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 711 (2011) ("Now suppose disclosees locate information, recognize its relevance and importance, and try to understand it. Many will fail.").

184. Boyd et al., *supra* note 35 ("Parents are clearly concerned about the risks and dangers that their children may face online even if they are simultaneously allowing them to lie about their age to get access.").

185. *See generally* Lewis Kornhauser, *Methods of Law and Economics*, *in* ENCYCLOPEDIA OF THE PHIL. OF L. AND SOC. PHIL. (M. Sellers & S. Kirste eds., 2020); Lewis Kornhauser, *The Economic Analysis of Law*, *in* STAN. ENCYCLOPEDIA OF PHIL. (Jan. 7, 2022), https://plato.stanford.edu/entries/legal-econanalysis/ [https://perma.cc/HP47-466S].

diminished, if not entirely eliminated, by shifting that burden to the first parties.

Since the current regulation is ineffective, something must be changed in order to protect children's information to the extent desired. This change must be statutory rather than a change in interpretation of the existing regulations in order to mandate compliance.[186] COPPA's insufficiencies can be rectified in six ways.

My first suggestion for how to better protect children's information given the expansive use of third parties is privacy by default. The idea of privacy by default is that companies would be required to implement the privacy protections required by COPPA but that there would be no additional steps for parents to take in setting up those protections; they would be implemented automatically, or "by default." Companies would be required to have the settings automatically at the most protective when first signing onto or using a service or device. A user could then opt into any sort of information sharing with third parties at their own desire.[187]

Given that privacy by default has already been suggested and has made little strides towards better protecting privacy, I would amend the suggestion to include a technology that distinguishes a child's voice from that of an adult. When the system picks up that a child is the one using the device, the greatest possible privacy protections would automatically kick in.

Privacy by default would avoid the burdensome requirements of parental consent because the greatest privacy protections possible would already be in place. This would also avoid the hurdle of trying to have children select the privacy settings they want when unsupervised by an adult. Given that children might not fully understand the need to protect their privacy or the consequences that come with using certain services, they are in heightened need for privacy by default. Such a solution is better than COPPA because COPPA only works toward its goal when children are closely supervised by adults and requires those adults to consent, and even then,

186. *See* ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 8 (Basic Books 1995) (advocating for a statutory change instead of changing the interpretation of the existing privacy laws).

187. Matecki, *supra* note 3, at 398 ("Websites with an 'opt-out' mechanism require users to take an affirmative step to protect personal information; for example, checking 'accept' to a statement allowing for the disclosure of private information to third parties. Opt-in policies, on the contrary, mandate that as a default option, personal information cannot be shared or disseminated with third parties *unless* a user affirmatively grants permission.").

not all sites are covered by the Act.[188] Privacy by default also avoids the assumption that COPPA requires that parents are more capable of making decisions.[189] As discussed above,[190] that is a poor assumption given that parents are unlikely to be fully informed about the details of data processing practices.[191]

Privacy by default can be implemented and enforced through legislation replacing or reinforcing COPPA. The suggestion takes into account the fact that parents are unlikely to read or become informed about their own transactions by putting the burden of privacy on the service itself. That way, by the time the parent is put in a place where they have to consent or make decisions about their child's information, they will know that their child is already being protected to the greatest extent possible. While privacy by default might have previously been proposed, it can be tailored to the protection of children's information in new ways, better supporting the aims of COPPA.

Second, under the cheapest cost avoider rationale, the FTC and COPPA should also be more diligent at enforcing privacy by design.[192] Privacy by design means that companies should build the privacy into the design of the service through anonymization and encryption of information and be punished when they either do not do so or do so inadequately.[193] Some other ways to incorporate privacy by design are through risk assessments of privacy or security, minimizing the amount of data collected and the length of time it

188. Allen, *supra* note 2, at 772 ("Now, as before COPPA's enactment, direct and constant parental supervision is needed to keep children from adult content, since most Web sites that do not collect personal information, and many that do, can be visited in part or in full by children of any age.").

189. van der Hof, *supra* note 30, at 434 (analyzing whether "the assumption that parents are more capable of making decisions than their children" is a fair one).

190. *See supra* Part V.

191. van der Hof, *supra* note 30, at 437–38 (reaching the conclusion that parents are not the best parties to make decisions about releasing their children's personal information online since parents most likely do not have information about the details of data processing practices).

192. *See* Forbrukerradet, Toyfail An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys 36 (2016), https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf [https://perma.cc/WNG4-ZYNY] ("[T]he NCC [(Norwegian Consumer Council)] suggests that manufacturers of connected toys adopt a design-philosophy of privacy and security by design. . . . This is also the way forward according to the European Commission and the Article 29 Working Party, and is codified in the new GDPR.").

193. Internet of Things: Privacy & Security in a Connected World, *supra* note 14, at iii ("[C]ompanies should build security into their devices at the outset, rather than as an afterthought.").

is retained for, and testing security and privacy measures before launching a product.[194] Privacy by design is distinguished from privacy by default because privacy by design works security practices into the system while privacy by default automatically has a user set at the highest level of possible privacy and security protection. While certain aspects of privacy by default can be specifically tailored towards children, privacy by design is a broader privacy protection that would be implemented for all users. Since children are subjected to greater dangers and risks from the leaking of their PII, as mentioned earlier,[195] they would inversely benefit from privacy by design protections more than adults who do not originally face such great risks. Security and privacy protections should be built into devices at the outset to prevent issues from arising instead of after an issue has already arisen.[196]

Not only would these protection measures prevent the compliance issues with COPPA, but they would also resolve the problems of third-party sharing since the third-party companies would also have privacy by default and an effective privacy by design system as part of their models. By the third party adopting the same level of privacy protection as the first party, children and their parents know exactly how the information will be used and stored without having to spend extensive amounts of time searching for and reading privacy policies. The economic cost of first parties monitoring third parties for compliance would also decrease, as the first parties could be ensured that the third parties are implementing the required precautions. Because of the decrease in costs, companies would likely support the new regulations, making them easier to implement and enforce. In thinking of a users' PII as a fundamental right and property interest, these policies should be adopted not only for children, but for adults as well.[197] Avoiding rules based on age or other demographic traits evades the unintended consequences such as the uncomfortable position parents are put in when having to choose "between curtailing their children's access and condoning lying."[198] It also evades the costs of requiring certain programs for only some companies by instating them across the board.

194. *Id.*

195. *See supra* Part I(B).

196. INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, *supra* note 14, at iii.

197. Ciocchetti, *supra* note 5, at 100 (showing how other proposed regulations treat PII as both a fundamental right and a property interest).

198. Boyd et al., *supra* note 35.

Third, the regulation could also have incentives built in to increase participation and compliance, if needed. Since rational businesses, under the law and economics theory, respond to incentives, that would increase and ease compliance with the law. Such incentives would result in furthering the goals of protecting children's information. For example, there could be monetary incentives for increased protections, above those required by the law or certifications displayed on a company's website or online platform demonstrating that they have exceeded the required security measures. In whatever way it takes to change the current frameworks, something must be done to prevent the lack of COPPA compliance from undermining the effectiveness of future regulations in the same realm.

Further suggestions include, fourth, data minimization, fifth, purpose limitations, and sixth, immediate deletion of a child's data. If regulators were to adopt data minimization, companies would only collect and store as much data as is absolutely required.[199] A purpose limitation would restrict the ways in which a company can use the data once they collect it so that parents can easily determine exactly how their child's data is being used without the burdensome searching.[200] Finally, companies should be required to delete children's data as soon as it is no longer needed.[201] The latter suggestion, though already included in COPPA, needs to be further highlighted to reach its full potential for protection since it does not seem to be happening in practice under COPPA.[202] Furthermore, first-party firms should be responsible for ensuring that all third-party services that are connected and accessible through the device provide complete and tailored privacy notices before use. Those notices, in addition to the privacy policies of the smart speakers themselves, can be audio clips that play before use. If the service

199. INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, *supra* note 14, at iv (defining data minimization as "the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it").

200. *See* FORBRUKERRADET, *supra* note 192, at 18–25 (arguing that there should be a purpose limitation for three different actions: (1) sharing data with third parties, (2) advertising toward children, and (3) further use of voice data).

201. *See* Emily McReynolds et al., *Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys*, PROCS. OF THE 2017 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS. (2017).

202. *Complying With COPPA: Frequently Asked Questions*, *supra* note 59 ("[T]he Rule specifically states that operators should retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected.").

being accessed is one that is directed to children, the audio clips can be specifically tailored to a child's comprehension level.

VI.
CONCLUSION

Many companies are not complying with COPPA requirements on their face. Those breaches are taken even further when children's personal information is shared with third parties who do not comply with the regulation. COPPA is not useful when the children's information is not being protected by the first-party firm which originally collects it. The analyses of Amazon's Alexa and the Google Home show how first parties who purportedly comply with COPPA share children's personal information with third parties. Those third parties who receive that information do not even attempt to comply, demonstrating the dangers that come with COPPA's failure to adequately address the relationships between first and third parties. There is a blind spot in COPPA when it comes to third parties that will threaten children's data in products and services far beyond just smart speakers and devices. To address this problem of unsecure child's data, policymakers and regulators should push for and adopt privacy by default in addition to privacy by design. Not only would such requirements restrict third-parties' access to the child's data which could then no longer be protected by COPPA, but they would reinforce the COPPA requirements on the first-party and third-party companies as well. Overall, privacy by default supports not only the protection of children's information but the business models of first parties who should otherwise be responsible for ensuring compliance, therefore minimizing costs for first parties.