LEANING INTO CHAOS (CHILD'S HEALTH AND ONLINE SAFETY ACT): REVISION TO FTC'S ENFORCEMENT OF COPPA & NEW MODEL RULE FOR CHILD ADVERTISING

Gabrielle N. Schwartz, J.D., CIPP/US

LEANING INTO CHAOS (CHILD'S HEALTH AND ONLINE SAFETY ACT): REVISION TO FTC'S ENFORCEMENT OF COPPA & NEW MODEL RULE FOR CHILD ADVERTISING

Gabrielle N. Schwartz, J.D., CIPP/US*

I. INTRODUCTION

A wise author once wrote, "I know, up top you are seeing great sights, but down here at the bottom we, too, should have rights."[1] Dr. Suess not only understood the importance of inspiring children, but believed it was essential to teach children valuable life lessons. As more children continue to stray away from reading as their source of entertainment, children are more likely to become fascinated by the beauty of the internet. Although the internet's capabilities may positively impact children, there are also adverse effects through the use of the internet's products, services, and content. Many companies, individuals (such as parents), and lawmakers are calling for action to be taken to prevent and protect against arguably toxic online content.

President Biden, in his recent State of the Union address, stated that although the Child Online Privacy Protection Act (COPPA) has "provided a solid foundation for supporting parent control,"[2] the evolution and change in the advertising techniques on the internet should influence the need to change and equip parents with updated resources "to ensure broad children's safety while addressing present-day challenges technologies are posing."[3] To accomplish this change, Congress must heed these warnings and pass a new comprehensive child privacy law that incorporates aspects of COPPA but also broadens the protection for one of the most vulnerable populations against the negative aspects of the internet.[4]

In this piece, I will first discuss the historical background of the Federal Trade Commission's (FTC's or the Commission's) authority to regulate child advertising. Second, I will illustrate how the current law, COPPA, regulates entities who direct their websites or online services and advertising to children. Next, I will provide case law that illustrates the weaknesses of COPPA. Finally, I will propose adopting a new model act, CHAOS (Child's Health and Online Safety Act), that would amend COPPA and strengthen the foundation to protect our vulnerable population. This new act would seek to replace the various shortcomings that COPPA has not

* Graduate, Class of 2023, University of Maine School of Law. This paper was previously included in the September 2022 edition of the *Student Journal of Information Privacy Law* (online publication) and is being republished as an article after receiving an additional round of editing.

1. DR. SEUSS, *Yertle the Turtle, and Gertrude McFuzz* (1979).

2. JOSEPH DUBALL, *Biden's State of the Union remarks put children's privacy front and center*, IAPP (Mar. 2, 2022), https://iapp.org/news/a/bidens-sotu-remarks-put-childrens-privacy-front-and-center/?mkt_tok=MTM4LUVaTS0wNDIAAAGC6tSEAKjRnd0Ya2SI2cu6jUFdZcE9GxIBJUYmZ9ZA9tQgRYfrTnutPFXuXxlMjFXR8S5oSEJTJcWKYevUCduHRfurbuQozbB4idUbqAZu0N4k/.

3. *Id.*

4. *Id.*

yet addressed and would require new broader obligations such as banning targeted advertising to children, stopping the collection of personal information from children in certain regards, and adopting a new scope, expanded definitions, education opportunities, and more that would provide a more appropriate level of protection for children.

II. BACKGROUND

A. Overview of the FTC's Enforcement Power

The evolution of technology and the power of social media, the internet, and smart devices have created a particularly open-world environment for children. More and more children can navigate this ever-evolving technology and are caught in a wave of new advertisements that prove smarter and craftier at gaining information. As society continues to understand the scope of this power, the FTC has a long history of attempting to regulate and enforce commerce with a focus on advertising and marketing practices. Specifically, the FTC has the authority to ensure that children are given meaningful protections against advertisements targeted to manipulate or deceive them.

The FTC's authority to regulate advertising and marketing practices stems from Section 5 of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful."[5] The Commission clarifies further that "a representation, omission, or practice is deceptive if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers – that is, it would likely affect the consumer's conduct or decisions with regard to a product or service."[6] On the other hand, an act or practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition."[7]

When interpreting whether a particular practice is considered unfair, the FTC looks at whether it is "immoral or unethical or offends public policy as established by statute, common law, industry practice, or otherwise."[8] Instead, the analysis for determining whether an act or practice is deceptive involves whether "(1) there is a representation, omission, or practice, that (2) is likely to mislead consumers acting reasonably under the circumstances, and (3) the representation, omission, or practice is material."[9] If the practice is targeted at a specific audience or group, such as children, the FTC "will determine the effect on a reasonable member of

5. 15 U.S.C. § 45(a)(1) (2011).

6. FED. TRADE COMM'N, *Commission Enforcement Policy Statement on Deceptively Formatted Advertisements,* (Dec. 22, 2015), https://www.ftc.gov/system/files/documents/public_statements/896923/151222deceptiveenforcement.pdf.

7. 15 U.S.C. § 45(n) (2011).

8. DEAN K. FUEROGHNE, *Law and Advertising: A Guide to Current Legal Issues*, 56 (Rowman & Littlefield 4th ed. 2017).

9. *Id.* at 40.

that group."[10] Therefore, it is essential to note that advertisements that target or are directed at children will be viewed from the standpoint of an ordinary child.

In addition, the FTC has the authority to regulate advertising that is considered to be false and emphasizes the need for truth-in-advertising standards. This specific subsect of advertising is regulated under the "deceptive advertising"[11] prong. Thus, advertisements to children must stay truthful and cannot confuse or mislead the child into believing that the product or service is free, safe, or does not state that it does or does not do something when it does the opposite.[12] As children become more engaged in the use of technology, operators of these websites or online services must take special care to ensure that children are not placed in a position where they cannot understand the scope of the information being collected and are not misled into revealing information in order to access a product or service.

B. COPPA: A Historical Overview

As a regulatory body that deals with consumer protection, the FTC enforces COPPA. The FTC's responsibility is to designate rules to protect children's privacy and their data, as well as to ensure that the decision-making power to disclose and protect children's data remains in the hands of parents. COPPA has been in effect since 2000, and the FTC revised the rule in 2013.[13] Currently, the law as written is directed to protect children under the age of thirteen and places a burden on website or online service operators to be aware of the various responsibilities under this rule.[14]

Under COPPA, the FTC has authority over any website or online service that directly targets children under thirteen, as well as sites that are "directed to a general audience or operate[s] an ad network, plug-in, or other third-party service used by kid-directed sites."[15] Specifically, the operator of that site or online service must have "actual knowledge" that they are collecting that information from children under thirteen.[16] Additionally, operators gain "actual knowledge" when "collecting personal information from users of another site or online service directed to kids under [thirteen]."[17] COPPA does not define the term "actual knowledge," but the 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."[18] Once it is determined that COPPA

10. FED. TRADE COMM'N, *FTC Statement on Deception,* 103 F.T.C. 3 (1984) (*appended to Cliffdale Assocs., Inc.,* 103 F.T.C. 110 (1984)) ("Deception Policy Statement"), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

11. *Id.*

12. *See id.*

13. *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013)*; see, e.g*, FED. TRADE COMM'N, *FTC's Children's Online Privacy Protection Rule: Not Just for Kids' Sites*, (Apr. 2013), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites.

14. *See id.*

15. *Id.*

16. *Id*.

17. *Id.*

18. *FTC's Children's Online Privacy Protection Rule*, *supra* note 13.

covers a certain website or online service, the operator must "post privacy policies, provide parents with direct notice of their information practices, and get verifiable consent from a parent or guardian before collecting personal information from children."[19]

To ensure that website or online service operators covered by COPPA disclose the necessary and relevant information regarding the potential collection of children's personal information, the operator must publish a privacy policy.[20] The privacy policy must "clearly and comprehensively describe how personal information collected online from kids under [thirteen] is handled" and further must "describe not only [the operator's] practices, but also the practices of any others collecting personal information on [the operator's] site or service."[21] COPPA states that the privacy policy must be posted as a link on the operator's "homepage and anywhere [the operator] collects personal information from children."[22] If the website or online service is directed to a general audience, instead of children, the operator must create a "separate section for [children and] post [the] link . . . [to] the homepage of the [children's specific section] of [the] website or service."[23] Particularly since children will be on a different reading level than most adult consumers, the privacy policy should be "clear and easy to read"[24] and must include "a list of all operators collecting personal information; a description of the personal information collected and how it is used; and a description of parental rights."[25] The operator is responsible for including the following information in the policy:

> [T]he types of personal information collected from children; how the personal information is collected – directly from the child or passively, or through cookies; how the personal information will be used; and whether [the operator] disclose[s] personal information collected from kids to third parties [and if so, the] privacy policy must then list the types of businesses [the operator] disclose[s] information to and how they use the information.[26]

Finally, the privacy policy must also notify parents of their rights under COPPA which include:

> [T]hat [the operator] won't require a child to disclose more information than is reasonably necessary to participate in an activity; that [the parent] can review their child's personal information, direct [the parent] to delete it, and refuse to allow any further collection or use of the child's information; that [the parent] can agree to the collection and use of their child's information, but still not allow disclosure

19. *Id.*; *see* 16 C.F.R. § 312.4.

20. *FTC's Children's Online Privacy Protection Rule*, *supra* note 13; *e.g.*, Federal Trade Commission, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business,* (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

21. *Children's Online Privacy Protection Rule*, *supra* note 20.

22. *Id.*

23. *Id.*

24. *Id.*

25. *Id.*

26. *Id.*

> to third parties unless that's part of the service; and the procedures to follow to exercise their rights.[27]

COPPA gives parents the power to control the collection and disclosure of their child's personal information. Therefore, it requires that the operator of a website or online service give parents "direct notice of the information practices before collecting information from their kids."[28] Similar to the privacy policy, the notice should be easily digestible and must tell parents the following:

> [T]hat the [operator] collected the parent's online contact information [to get] their consent; [the operator] want[s] to collect personal information from their child; that [the parent's] consent is required for the collection, use, and disclosure of the information; the specific personal information [the operator] want[s] to collect and how it might be disclosed to others; a link to [the] online privacy policy; how the parent can give their consent; and that if the parent doesn't consent within a reasonable time, [that the operator will] delete the parent's online contact information from its records.[29]

Once an operator provides direct notice to parents, the next step is to allow parents to provide verifiable consent before collecting, using, or disclosing information from a child.[30] COPPA provides that there are various acceptable methods, including having the parent:

> [S]ign a consent form and send it back via fax, mail, or electronic scan; use a credit card, debit card, or other online payment systems that provide notification of each separate transaction to the account holder; call a toll-free number staffed by trained personnel; connect to a trained personnel via a video conference; provide a copy of a form of government-issued ID that you check against a database, as long as [the operator] delete the identification from the records when [the verification process is finished]; answer a series of knowledge-based questions; or verify a picture of a driver's license or other photo ID and then comparing that photo to a second photo submitted by the parent, using facial recognition technology.[31]

COPPA encourages various methods and states that if the child's personal information is used for internal purposes only, the operator may use a method known as "email plus."[32] Under this method, the operator will "send an email to the parent and have them respond with their consent,"[33] and the operator must "send a confirmation to the parent via email, letter, or phone call."[34] Regardless of what method the parent uses, the operator must "let the parent know that they can revoke their consent at anytime."[35] The operator must also "give parents the option of allowing the collection and use of their child's personal information without

27. *Id.*
28. *Id.*
29. *Id.*
30. 16 C.F.R. § 312.5.
31. *Children's Online Privacy Protection Rule*, *supra* note 20; *see* 16 C.F.R. § 312.5.
32. *Id.*
33. *Id.*
34. *Id.*
35. *Id.*

disclosing that information to third parties."[36] There are a few narrow exceptions to the general rule regarding parental consent before collecting a child's personal information, but the operator may still "have specific notice requirements."[37]

Not only do parents have rights regarding their child's personal information before it is collected or disclosed, but they also have ongoing rights that the website or online service operator must continue to honor.[38] Parents have the right to request, and the website operator must honor the following: 1) give parents a way to review the personal information collected concerning their child; 2) give parents a way to revoke their consent and refuse the further use or collection of personal information; and 3) delete their child's personal information.[39] The operator has a continuing obligation to ensure that any communication is with the child's parent[s] and that it is not "unduly burdensome" on the parent to exercise their rights.[40]

Finally, COPPA requires that the operator "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information from children."[41] COPPA states that the operator should minimize collection of data in the first place and "take reasonable steps to release personal information only to service providers and third parties capable of maintaining its confidentiality, security, and integrity."[42] Further, the operator should only retain information "as long as reasonably necessary for the purpose for which it was collected"[43] and must "securely dispose of it once [the operator] no longer has a legitimate reason for retaining it."[44] Although the FTC maintains regulatory and enforcement power over COPPA violations, the Commission may rely on guidance and high-level principles to ensure the highest level of protection against deceptive and unfair advertising.

C. ICPEN Best Practice Principles

The International Consumer Protection and Enforcement Network (ICPEN) is a vital organization consisting of consumer protection authorities from over 65 countries, whose aim is "to protect consumers' economic interests around the world, share information about cross-border commercial activities that affect consumer welfare, and encourage global cooperation among law enforcement agencies."[45] The FTC is a member of ICPEN, and although these principles are not binding, it is essential to review the updated best practices principles created by

36. *Id.*
37. *Id*.
38. *Id.*, *see* 16 C.F.R. § 312.6.
39. *Id.*
40. *Id.*
41. *Id.*, *see* 16 C.F.R. § 312.8.
42. *Id.*
43. *Id.*
44. *Id., see* 16 C.F.R. § 312.10.
45. ICPEN, *Best Practice Principles: Marketing Practices Directed Towards Children Online*, (June 2020), https://icpen.org/sites/default/files/2020-06/ICPEN%20-%20Best%20Practice%20Principles%20for%20Marketing%20Practices%20Directed%20Towards%20Children%20Online%202020.pdf.

ICPEN to understand the "range of issues that concern consumer protection agencies and the variety of approaches they use to ensure marketing to children online complies with the laws in their jurisdictions."[46] The increasing level of children's activity online has sparked a heightened interest in regulating advertisements to prevent undue harm and manipulated marketing practices.

The principles created and updated by ICPEN are based on the results of a survey that ICPEN members completed in 2018.[47] The responses gathered and analyzed by ICPEN revealed four key issues that are of concern:

> 1) the lack of transparency when commercial and non-commercial content are mixed; 2) marketing practices that exploit children's lack of commercial knowledge, naivety, and credulity; 3) the lack of transparency concerning the processing of children's data and using children's data in personalized ads; and 4) marketing inappropriate products to children.[48]

When applying these principles, understanding the advertisement's audience is critical, specifically whether the content is directed towards children. ICPEN states that traders should consider the following factors in determining whether their content is directed towards children: "a) the nature of the marketing content; b) the placement and audience; and c) the product or service."[49] ICPEN clarifies that the definition of "child" varies across jurisdictions and, therefore, has decided that for these principles, "a child is a person under the age of [eighteen]."[50] These principles prevent undue harm posed by direct marketing to children online and encourage transparency in how children's data is collected and disclosed.

D. Recent Cases

As technology has evolved to become more invasive, advertising and marketing practices have progressed to become more ingrained in the daily online activities of children. This progression has signaled to the FTC that there needs to be more enforcement and regulation, yet there are still companies that can deceive or unfairly harm children through their advertisements. Therefore, under Section 5 of the FTC Act, the FTC has the enforcement power to ensure that companies that violate COPPA and Section 5 are held accountable. These cases showcase that although COPPA is a great starting point in ensuring that children are protected against deceit and manipulation, there are still many steps to be taken before parents can breathe easily.

One such case involves OpenX, a company that operates a programmatic advertising exchange designed to use real-time bidding to help "publishers of Web

46. Stacy Feuer, *Navigating the world of kids' marketing: Best Practice Principles from ICPEN*, (Aug. 17, 2020), https://www.ftc.gov/business-guidance/blog/2020/08/navigating-world-kids-marketing-best-practice-principles-icpen.

47. ICPEN, *supra* note 45.

48. *Id.*

49. *Id.*

50. *Id.* (ICPEN has noted that this age is established by Article 1 of the UN Convention on the Rights of the Child (1989)).

sites and mobile applications monetize their properties through advertising."[51] The FTC alleges that OpenX violated COPPA due to its collection of personal information from children under thirteen without parental consent.[52] The FTC's investigation found that "OpenX reviewed hundreds of child-directed apps with terms that identified the intended audience as 'for toddlers,' 'for kids,' 'kids games,' or 'preschool learning,' and included age ratings for the apps indicating they were directed to children under [thirteen]."[53]

Although OpenX stated that they had a support team to review each application, "these apps and their data were not flagged as child-directed and participated in the OpenX ad exchange."[54] The FTC, therefore, stated that OpenX had violated COPPA "because OpenX had knowledge that apps in the ad exchange were child-directed and that the company was collecting personal information from children under [thirteen]."[55] Additionally, "OpenX passed this personal data to third parties that used it to target ads to users of the child-directed apps."[56] As a consequence, OpenX agreed to a two million dollar settlement, and the "order requires OpenX to delete all ad request data it collected to serve targeted ads and implement a comprehensive privacy program to ensure it complies with COPPA and stops collection and retention of personal data of children under [thirteen]."[57] To maintain compliance, OpenX is required to "re-review apps on a periodic basis to identify additional child-directed apps and ban them from the company's ad exchange."[58] Lastly, OpenX must "keep track of which apps and websites have been banned or removed from its exchange."[59] This case further accentuates the issue that children face unknown harm from companies through advertisements, which shows an increased need to prevent collecting sensitive personal information online.

Children are becoming more active on the internet, leading many platforms and websites to market, promote, and incentivize their products or services to children. This, in turn, has collected vast amounts of information without the children's or parents' knowledge or consent. An example of this dilemma is shown in *FTC v. Google*, which illustrates when a company has actual knowledge that they have children using their website yet did not make any effort to comply with COPPA. The FTC entered into one of its most comprehensive settlement agreements, relying on COPPA, against YouTube in September of 2019, and has

51. U.S. v. OpenX Tech., Inc., No. 2:21-cv-09693, 2021 WL 6621824, at *4 (C.D.Cal.Dec. 15, 2021).

52. *Id.* at 13.

53. FED. TRADE COMM'N, *Advertising Platform OpenX Will Pay $2 Million for Collecting Personal Information from Children in Violation of Children's Privacy Law*, (December 15, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/12/advertising-platform-openx-will-pay-2-million-collecting-personal-information-children-violation.

54. *Advertising Platform OpenX*, *supra* note 53.

55. *Id.* at 2.

56. *Id.*

57. *Id*.

58. *Id.*

59. *Id.*

showcased that, ultimately, there needs to be added protections against large online platforms that can reach millions of children worldwide.

YouTube is an online video-sharing platform on which consumers can view videos and upload their own video content to share with others.[60] YouTube does not require users to register or create an account before viewing videos, but as a result, this limits the activities one can do, such as commenting on videos.[61] If an individual wants to create a Google or YouTube account, they must provide their "first and last name, e-mail address, and date of birth,"[62] and those who identify as under thirteen are prohibited from creating an account.[63] Once a user has created an account, the user may also make their own channel to upload videos.[64] Even further, users are encouraged to set "key words" that would allow "other users searching for videos on YouTube [to] find their channel."[65] Although YouTube is free to use, channel owners can monetize their channel by allowing the use of advertisements on their video[s], which in turn earns revenue.[66]

YouTube's content directly falls under the purview of COPPA due to the marketing and promotion of children's products and services, making them a top destination for kids.[67] The FTC held that despite YouTube continuously asserting that they do not need to comply with COPPA, YouTube falls squarely within the definition of "child-directed," as they have actual knowledge that children use their platform.[68] Further, not only does YouTube have a separate application called YouTube Kids, but they also host numerous channels that are "directed to children."[69] YouTube has this direct knowledge because the service works and communicates directly with many of these child-directed channels and even determines what content on specific channels is child-directed.[70] YouTube and Google have both "automated and manual means to review channels and videos on YouTube and assign them specific content ratings."[71] Consequently, those channels that are intended for children must comply with COPPA. At no point in time did YouTube attempt to gain verifiable parental consent from children viewing child-directed channels, thus securing personal information from unaware children and parents who were not given any notice as required under COPPA.[72]

The advertisements placed on these child-directed channels exemplify a larger problem: any online platform or website can, under the radar, potentially collect millions of dollars of revenue by exploiting children. The FTC complaint revealed

60. Complaint at 6, FTC v. Google, LLC., No.: 1:19-cv-02642 (D.D.C. Sept. 4, 2019).
61. *Id.*
62. *Id.*
63. *Id.*
64. *Id.* at 7.
65. *Id.*
66. *Id.*
67. *Id.* at 8.
68. *Id.* at 10.
69. *Id.*
70. *Id.* at 9.
71. *Id.*
72. *Id.* at 16.

that "YouTube earned nearly $50 million,"[73] and the targeting of children led to ultimately higher total ad counts than the targeting of adults.[74] The suit spawned a $170 million judgment against YouTube, which will not "make much of a financial dent in the company's deep pockets."[75] As this settlement illustrates, the FTC is constrained by its own regulatory body to "levy relatively small penalties on companies for violating consumers' privacy,"[76] but has shown that other potential enforcement mechanisms, such as changing ones' privacy policy and procedures, can prove to be slightly more effective.[77] How COPPA is written currently, and the enforcement procedures utilized by the FTC, continue to raise the question of whether COPPA needs to be amended to prohibit this exact activity in the first place. A new law needs to be developed and implemented to deter the invasive and illegal collection of children's personal information using advertisements.

III. LOOKING FORWARD: MODEL RULE

A. Purpose, Scope, and Definitions

In the last few years, parents and children have faced considerable changes on the internet, specifically with what children are exposed to. There are additional consequences stemming from the COVID-19 pandemic and its effect on the use of social media, online websites, or platforms. The youth mental health crisis is exacerbated by the use of these platforms, which "for years have been conducting a national experiment on our children and using their data to keep them clicking, with enormous consequences."[78] While the internet can be beneficial in many ways, it can also "reinforce negative behaviors like bullying and exclusion, and undermine the safe and supportive environments young people need and deserve."[79] Due to this extremely harmful effect on children, this paper addresses the need to call on Congress to strengthen privacy protections for children by banning targeted advertising to children, stopping the collection of personal information from children (in certain situations), and adopting a new model Act (CHAOS) that will amend COPPA to strengthen the foundation to protect our vulnerable populations.

---

73. Stuart Cobb, *It's Coppa-Cated: Protecting Children's Privacy in the Age of Youtube*, 58 Hous. L. Rev. 965, 975 (2021). *E.g.*, FED. TRADE COMM'N, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, (Sept. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law.

74. Cobb, *supra* note 73, at 975.

75. *Id.*

76. *Id.*

77. *Id.*

78. THE WHITE HOUSE, *FACT SHEET: President Biden to Announce Strategy to Address Our National Mental Health Crisis, As Part of Unity Agenda in his First State of the Union*, (Mar. 1, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/01/fact-sheet-president-biden-to-announce-strategy-to-address-our-national-mental-health-crisis-as-part-of-unity-agenda-in-his-first-state-of-the-union.

79. *Id.* at 1.

One of the most significant revisions to COPPA to be included in CHAOS is amending the definition section, specifically focusing on how "children" and "website or online services" are defined. The new model rule would amend COPPA to include "children under the age of [eighteen],"[80] perhaps with a subsection defining persons under the age of [fourteen] to be "children" and another "young people" or "teenager" subcategory that includes persons from 15 – 18.[81] COPPA currently only protects children under thirteen, which does not provide reasonable safeguards for children because persons under eighteen experience vulnerabilities that need to be protected depending on age and various other demographic factors.[82]

Other proposed legislations have capped the age limit to sixteen, but this does not consider the full range of diverse mental associations and experiences that influence a person's decision until the age of eighteen. Further, persons under eighteen are "generally considered more at risk from harmful marketing practices due to their lack of experience, credulity, and relative lack of understanding of commercial practices."[83] This would also allow added protections against social media companies, who argue that COPPA does not apply because "many require users to be at least [thirteen] years old to sign up"[84] and would prevent the need for children under thirteen to lie about their age to use social media or other online platforms.[85]

The model rule would also broaden the scope to whom the law applies to ensure that any company that could potentially collect children's personal information would be required to comply. Although COPPA defines "website or online service" somewhat broadly, CHAOS would not only include standard websites but would also apply generally to all online services "provided for remuneration – including those supported by online advertising – that process the personal data of and are likely to be accessed by children under [eighteen] years of age, even if those services are not targeted at children."[86] By broadening this definition, the Act would bring "apps, search engines, social media platforms,

80. U.K. INFO. COMM'RS OFF., *Age Appropriate Design: A Code of Practice For Online Services*, at 17, (Sept. 2, 2020), https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf; *e.g.,* Protecting the Information of our Vulnerable Children and Youth Act, H.R. 4801, 117th Cong. § 2 (2021-2022); *see also* ICPEN, *supra* note 45).

81. ICPEN, *supra* note 45 (ICPEN gives guidance that other countries do this. In this paper, we will use both "child," "children," and "teenagers" interchangeably as a means to identify persons under the age of 18.).

82. *Id.* at 5.

83. *Id.*

84. Rachel Lerman, *New bill would update decades-old law governing children's privacy online, add protection for teens*, WASHINGTON POST (July 29, 2021), https://www.washingtonpost.com /technology/2021/07/29/coppa-update-teenagers-online/.

85. *Id*.

86. Nancy Libin and Alexander B. Reynolds, *New Children's Data Privacy Protections Take Effect in the U.K.: What to Know and How to Comply*, DAVIS WRIGHT TREMAINE LLP BLOG (Sept. 1, 2021), https://www.dwt.com/blogs/privacy--security-law-blog/2021/09/uk-child-data-protection-laws. *See* JDSUPRA, *New UK Standards for Children's Digital Services Take Effect — Provides Framework for New US Law*, (Sept. 24, 2021), https://www.jdsupra.com/legalnews/new-uk-standards-for-children-s-digital-9874201/

online games and marketplaces, news or educational websites, content streaming services, online messaging services," and others into the realm of compliance.[87] This particular definition would go hand in hand with the updated standard of how to define whether a company is a "website or online service," precisely due to a change in the knowledge standard required and which type of services apply.

To determine whether a company is a "website or online service" collecting personal information from children, COPPA looks at whether an operator of a website or online service is directed to children and if it collects personal information from them. This standard showcases whether an entity maintains "actual knowledge" that it is "collecting or maintaining personal information from a child."[88] COPPA does not consider all the methods of technologies available to the operators of these services or sites, thereby limiting the number of entities complying with this rule. Therefore, CHAOS would replace the actual knowledge standard with a "constructive knowledge" standard.[89]

By adopting this new standard of "constructive knowledge," potential operators may have constructive knowledge when "data is being collected from a child if that operator directly or indirectly collects, uses, profiles, buys, sells, classifies or analyzes (using an algorithm or other form of data analytics) data about the ages of users or to determine whether an online platform's content is directed to a particular age range."[90] CHAOS would also allow an inference of constructive knowledge from data obtained through "reports received under self-regulatory guidelines, complaints from parents or third parties, internal communications (such as documents about advertising practices, insertion orders, or promotional material to marketers), publicly available information, or communications to an ad network that content is intended for users of a particular age."[91] This expansion within CHAOS directly addresses situations in which companies may collect personal information from a child but do not direct their platform to children or may not have actual knowledge of the collection of personal information from children.

Part of this transition to a new standard of knowledge will also be to develop which specific factors the FTC will use to consider whether a site or service is directed to children. CHAOS would include not only those factors enumerated under COPPA but would also include "the language or other characteristics used on the website or online service, the placement of the marketing, whether children are likely to constitute a significant portion of the overall audience, and competent and reliable empirical evidence regarding audience composition."[92] As CHAOS intends to include the most significant protections for children, adding these factors will provide the FTC with more tools to determine whether a site or service is directed

87. Libin & Reynolds, *supra* note 86.

88. 16 C.F.R. § 312.3.

89. Children and Teens' Online Privacy Protection Act, S. 1628, 117th Cong. § 2(2) (2021-2022).

90. *Id.*

91. *Id.*

92. CHILDREN'S ADVERTISING REVIEW UNIT, *Self-Regulatory Guidelines for Children's Advertising*, (July 29, 2021), https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/caru_advertisingguidelines.pdf. *E.g.*, ICPEN, *Best Practice Principles: Marketing Practices Directed Towards Children Online*, (June 2020).

to children. Additionally, the FTC will gain more use of a law designed to protect children's personal information through an expansion of what is included in the definition of personal information.

COPPA currently includes the definition of "personal information," which is extremely limited to a set of identifiable information about an individual collected online. CHAOS would amend COPPA by not only adopting COPPA's definition but would also expand to include information that is "linked or reasonably linked to a specific individual or specific consumer device of a teenager or child."[93]

> As such, the actual definition will incorporate information that may include actual or perceived race, religion, sex, sexual orientation, sexual behavior, familial status, gender identity, disability, age, political affiliation or national origin; commercial information; biometric information; device identifiers such as digital fingerprinting; education information; health information; facial recognition information; contents of, attachments to, and parties to information such as e-mail, text message, voicemails, audio and video conversations; financial information such as bank account numbers, credit or debit card numbers, or insurance policy numbers; and any inferences drawn from the information described . . . in this definition to create a profile about the teenager or child.[94]

As many privacy laws are becoming signed and adopted into law, CHAOS incorporates the standard definition of personal information that would align child privacy to the current protection of adults.[95] By creating a linear and more well-rounded law protecting children's privacy and wellbeing, CHAOS will begin to change the way companies design their websites or online services and will be cautious before deciding to collect vulnerable personal information.

B. Collection of a Child's Personal Information

CHAOS incorporates transparency and education for children as a significant component in order to create a safe and enjoyable environment for children on the internet. Presently, COPPA does not include the burden for websites or online services operators to ensure processes that would clarify what is and what is not marketing. CHAOS will require operators not to use marketing techniques that exploit "children's naivety, credulity, or lack of commercial knowledge."[96] To achieve this, operators will not be allowed to participate in the "deceptive or harmful collection and use of children's data."[97] The online world is growing rapidly, and so are the various advertising techniques available to operators. CHAOS takes a step further than COPPA and will require that operators refrain from engaging in specific practices such as "native marketing," "like and share or

93. Protecting the Information of our Vulnerable Children and Youth Act, H.R. 4801, 117th Cong. § 9 (2021-2022).

94. *Id.*

95. *Id.* (CHAOS would also discuss what is not personal information, such as "deidentified information" or "information that is processed solely for the purpose of employment of a teenager.").

96. ICPEN, *Best Practice Principles: Marketing Practices Directed Towards Children Online*, (June 2020).

97. *Id*. at 13.

prize-winning activities," deceptive "in-game advertising," "targeted and personalized ads," and "profiling of children."[98]

As young members of the population, children and teenagers often lack the commercial experience to "differentiate between what is an ad and what is not."[99] One generally used advertising method on social media is "native marketing," where "adverts are designed to match the form and function of the platform on which they appear."[100] These ads are designed to carry "a tag identifying them as paid endorsements or sponsored content," but the way that children view these advertisements showcase a critical issue: "they appear alongside and share the look and feel of search results, tweets, status updates, photos, videos, or other content."[101] Some of those specific disclosures are "not conspicuous or placed where relevant."[102] Consequently, the line between what is an ad and what is not is heavily blurred. This ambiguity may easily persuade children to alter their behavior and lead to forced interaction with promotional content. Since this type of digital advertising is extremely popular on sites like Facebook, CHAOS would ban operators from using this marketing technique on children.

Social media, such as Facebook, Instagram, and TikTok, are often built around "influencers" or individuals who have gained celebrity status online, on TV, in movies, or in the news. Children and teenagers are among the largest audiences of these influencers and are easily persuaded to imitate, copy, or recreate the content they see online. Due to this particular hold over children and teenagers, many operators will also pay "influencers to advertise on their behalf in exchange for free products, services or discounts in return."[103] The reason for concern is that children follow these influencers for their personal content, making it difficult to discern what is an advertisement or not and whether the advertisement is a personal recommendation. Namely, children and teenagers will act on these distracting advertisements that glorify discounts or promotional codes, and in exchange, these influencers receive a commission. This type of non-disclosure or even deceptive advertising is easily distinguishable by adults, but children and teenagers might find it particularly difficult to understand that content is an advertisement. The need to ban this advertising technique will directly protect children from the exploitation of social media and the digital world's need to promote products or services.

Ever seen a shared post or tagged someone in a post to win a prize? Like and share or prize-winning activities are another way to expand the reach of advertisements and will typically focus "on the prize instead of the commercial message,"[104] which will "easily distract children's attention and engagement."[105] This apparent deception falls under the premise that children are now directly part of the operator's marketing strategy, praying on the innocence of a child to "more easily spread [ads] via the child's networks of friends and followers on social

98. *Id.* at 8.
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.* at 9.
105. *Id.*

media."[106] Children are a trusting population, and CHAOS will protect children's well-being, trust, and susceptibility to manipulation by restricting an operator's ability to use like and share or prize-winning activities. The operator must clearly disclose and tag in a bright-colored and large font that this post or content is an advertisement. In the scenario that the operator can showcase that the content is not intrusive through the collection of unnecessary information or manipulating a child into participating in a competition, buying a product, or signing up for a service. In this case, an operator can utilize this advertising technique.

In addition to social media, one of the most prominent activities children engage in online is games. CHAOS will address certain in-game advertising that will be considered deceptive or unfair, and ban such advertising from being used on children. In-game advertising is commonly used, and although it can be beneficial for entities and operators, this specific type of advertising blurs the line between what is and what is not an ad. In-game advertising can use "product placement where items within the game, such as cars, clothes, weapons, and drinks are branded."[107] These advertisements may also be included as part of the "game's scenery, which reward children with virtual money if a commercial is watched, or can even be in the form of pop-ups with difficult cancel buttons."[108] Children and teenagers have "less developed motor skills"[109] than adults, and this type of advertising forces children to interact with commercial and product information whether or not they want to. CHAOS will prohibit operators from using deceptive in-game advertising techniques and exploiting children who are unknowingly buying unnecessary products or spending large amounts of money without the knowledge or consent of their parents or guardian.

As advertising becomes more sophisticated and ingrained within apps, social media, and experiences that children engage with online, there is a heightened need for enhanced protection against children's personal information being collected and used against them for marketing purposes. Targeted advertising embodies a new wave of intrusive and disturbing data collection practices that can be easily deceptive and unfair towards children. Targeted advertising relies on "information about the viewer's preferences, which may be based on search and browsing history, purchase history, or social media activity."[110] CHAOS would make it unlawful for any operator to:

> Use, disclose to third parties, or compile personal information of a child for purposes of targeted marketing if 1) the child is a user of a service, and that service's operator has constructive [or actual] knowledge that personal information is being collected from children, or 2) the service is directed to a child.[111]

Thus, by effectively banning targeted advertising, children are protected from the monetization of data and the hostile and aggressive eye of the internet.

---

106. *Id.*
107. *Id*.
108. *Id.*
109. *Id.*
110. *Id.* at 13.
111. Children and Teens' Online Privacy Protection Act, S. 1628, 117th Cong. (2021-2022).

C. Privacy-by-Design, Disclosures, and New Standards

The underlying premise behind CHAOS is creating a new way of approaching and regulating the collection of a child's personal information to ensure the child's best interest, not the businesses. Although some new bills and proposed legislation create guidelines that operators may follow, CHAOS understands that to see change, a new set of standards must be created to ensure adequate protection for children against internet harm. Therefore, the following design standards must be considered by operators to ensure compliance with CHAOS. If not adhered to, these standards are binding and will be viewed as unfair and deceptive, as defined in Section 5 of the FTC Act.

First, a website or online service operator must follow a privacy-by-design standard to ensure that data processing is in the child's best interest.[112] To achieve this, operators must take steps to place the child's interests as the "primary consideration when . . . design[ing] and develop[ing] online services likely to be accessed by a child."[113] As the concept of privacy-by-design grows in the U.S., operators should design and deliver services in a way that protects children from exploitation and other harms that occur online.[114] This does not mean that operators cannot pursue their commercial interests, but instead must consider the way the platform is designed or viewed by a child to prevent the unnecessary, deceptive, or unfair collection of children's personal data.

Second, before an operator can collect or process any child's or teenager's personal information that is likely to result in a high risk to rights or freedoms, a "data protection impact assessment"[115] must be conducted to "assess and mitigate risks to the rights and freedoms of children who are likely to access this service."[116] To accomplish this assessment, the operator must take into account the "privacy and security risks, the rights and best interests of children and teenagers, differing ages, capacities, developmental needs of children and teenagers, and any significant internal or external emerging risks."[117] Further, to conduct the data protection impact assessment, the operator must consider, identify, and mitigate "any potential harm the processing would cause, including social anxiety, access to harmful content, excessive screen time, and other significant economic, social, or developmental disadvantage."[118] This risk assessment would go hand in hand with the privacy-by-design requirement because the operator must embed this assessment into the design process of the website or service "before the launch of the service and on an ongoing basis, and before making significant changes to the processing of covered information."[119] This inclusion will allow operators to create

112. *See Age Appropriate Design*, *supra* note 80.

113. *Id.* at 13.

114. *See id.*

115. Protecting the Information of our Vulnerable Children and Youth Act, H.R. 4801, 117th Cong. § 2 (2021-2022) (Or privacy and security impact assessment and mitigation).

116. *Age Appropriate Design*, *supra* note 80.

117. H.R. 4801, 117th Cong. § 2 (2021-2022).

118. *Age Appropriate Design*, *supra* note 80, at 30.

119. H.R. 4801, 117th Cong. § 2 (2021-2022).

an excellent foundation for the protection of children and ensure continuous monitoring of these protections.

Third, in addition to the privacy policy and notice or disclosure requirements under COPPA, CHAOS would also include certain standards that operators must adhere to, such as "providing adequate transparency; avoiding detrimental uses of data; developing default settings for high-level privacy protection; ensuring data minimization; limiting data sharing; providing enhanced protection for geolocation information; ensuring compliance of connected toys and devices; and providing online tools"[120] for both children and parents. These well-rounded standards begin with the inclusion of a "just-in-time notice" by the operator at the moment of data collection and will encourage children to speak to a parent or guardian before authorizing "any new use[s] of their data."[121] Although COPPA has privacy policy and notification requirements, this specific provision will ensure that ongoing compliance is met and that both parents and children are apprised of the collection and processing of information. Further, detrimental uses must be avoided, meaning that operators must not process children's personal data in ways that could be harmful to their health and wellbeing.[122] As mentioned previously, this will go hand in hand with the privacy-by-design and assessment requirements to ensure that the child's welfare is protected from the toxic harms of the internet.

Moreover, operators should create websites or online services that provide enhanced protections for collecting and processing children's personal information. One such example is "geolocation options must be turned off by default" or "must be an obvious sign when location tracking is active."[123] Sensitive information must be protected, and these controls would provide both parents and children more control over the possession of their information. Nowadays, there is such a variety of connected devices and toys that were not considered when COPPA was initially enacted, which should now play a more significant role in determining the proper protections for children. Under CHAOS, operators must provide effective tools to enable compliance that can be tailored to the child's age.[124] These online tools are expanded to include ways that children can exercise their rights and report concerns.[125] CHAOS will change the way operators will need to think about their website or online service available to children and create more rights and freedoms for children to truly enjoy the benefits of the internet.

Finally, CHAOS will create a new right of erasure, in addition to those codified by COPPA, that will mirror many current privacy laws. This new right will provide parents, children, and teenagers with a mechanism "to erase or otherwise eliminate content or information . . . [that they have provided to the service when such content] contains or displays personal information of children [or teenagers]"[126] and that service has made it "publicly available through [its]

120. *Age Appropriate Design*, *supra* note 80*; see* JDSUPRA, *supra* note 86.
121. *Id.*
122. *See* H.R. 4801, 117th Cong. § 2 (2021-2022).
123. JDSUPRA, *supra* note 86.
124. *See id.*
125. *See id.*
126. S. 1628, 117th Cong. (2021-2022).

website."[127] Although COPPA encourages data minimization and honoring future requests by parents regarding the information collected and processed internally or to third parties, this right will target information publicly posted on the platform. This will more precisely target social media platforms and give heightened privileges to parents and children when it comes to what information they want available on the internet. CHAOS creates these standards to safeguard minors through a safe online ecosystem. Compliance and enforcement of this act will become of the utmost importance to secure an easy transition or rollout of this law.

D. Enforcement

As mentioned previously, the FTC has been the primary regulatory body enforcing COPPA. With CHAOS replacing COPPA, there needs to be a specific reflection on whether the FTC can take on this enormous task of ensuring that all operators comply with the law. This will include continuously monitoring and enforcing actions against entities and operators who engage in deceptive and unfair acts against children. Therefore, CHAOS considers this and will require a new division to be created within the FTC known as the Youth Privacy, Marketing, and Wellbeing Division.[128]

The Youth Privacy, Marketing, and Wellbeing Division will be responsible for tackling and addressing the privacy and safety of children and teenagers. The FTC will appoint a Director who will head the division, who then must hire "adequate staff to carry out the duties,"[129] including but not limited to "individuals who are experts in data protection, digital advertising, data analytics, youth development,"[130] and psychologists who have expertise with children and teens. The division will be responsible for the advertising and marketing practices directed at children and teenagers. The division will also be required to submit yearly reports to the Committee on Health, Education Labor, and Pensions of the Senate and the Committee on Education and Labor of the House of Representatives. The report will include:

> 1) a description of the work of the [Youth Privacy, Marketing, and Wellbeing Division] on emerging concerns relating to youth privacy and marketing practices [as well as harms over the internet]; and 2) an assessment of how effectively the Commission has, during the period for which the report is submitted, addressed youth privacy and marketing practices [as well as child and teenager wellbeing].[131]

Although this Division's primary concern will be regulating children's and teenagers' interaction with the online sphere, the Division will also generate and maintain governmental funding for schools across the nation to establish educational opportunities to teach children how to navigate the internet. This funding will be explored and developed by the Division no later than one year after

127. *Id.*

128. *Id. See* H.R. 4801 (Both Acts call for a new Youth Privacy and Marketing Division to be established at the FTC.).

129. H.R. 4801, 117th Cong. § 2 (2021-2022).

130. *Id.*

131. *Id.*

the date of the enactment of this Act. Accordingly, it will be used to provide educational resources, tools, videos, or training geared toward children and teenagers. The Division is tasked with ensuring that operators of the website or online services change their behavior, and that children are equipped with the tools and techniques to navigate the internet. As society evolves and technology is even more pervasive in our youth's lives, the FTC must be responsible for ensuring that proper resources are allocated to our schools.

IV. CONCLUSION

Society and technology have heavily evolved; shouldn't the law advance with the everchanging environment we live in? Although COPPA has provided a strong foundation regarding children's privacy, the world has drastically changed since 2013. The law is no longer suitable to ensure the highest protection for children on the internet. Children are ditching books and outdoor games for YouTube, online games, and social media. The beauty of the internet allows children to experience and grow through its websites and online services, but can also be a source of hate, bullying, harmful content, and perpetual harm that can severely impact the development of both children and teens.

Therefore, it is Congress's responsibility to adopt a new law, CHAOS, that will broaden and expand the protections for children and allow the FTC more regulatory power. CHAOS seeks to change how advertising and marketing practices are designed to give parents the relief that their children's best interests are in mind. CHAOS will create a new wave of the internet by creating these new standards, redefining key concepts, and tailoring enforcement of unfair and deceptive acts. Not only will the internet become a safer environment for children and teenagers, but minors will now be equipped with the proper knowledge and tools to navigate their online experiences. I call on Congress to adopt CHAOS and answer the call by lawmakers, parents, the President, and others to enhance the privacy protections for our most vulnerable population and create a new generation of tech-savvy and safeguarded youth.