MOVING THE UNITED STATES INTO THE 21ST CENTURY FOR CHILDREN'S ONLINE PRIVACY RIGHTS

Zackary A. Blanton[*]

Abstract

It has been more than twenty-five years since the Children's Online Privacy Protection Act (COPPA) was first implemented in the United States. Since its enactment—well over a decade ago—there has been only one instance in which Congress successfully passed noteworthy modifications to the Act. While there has been a recent increase in proposed amendments to the Act better to protect children in our current reality of everchanging technology, little has been done to initiate the much-needed change. The increased focus on children's online rights has been sparked primarily by changes made in the United Kingdom. At the forefront of the drive for greater protection of the privacy rights of children, the United Kingdom's transformation has left the world considering what alterations need to be made to their current systems to stay up to date with this growing demand.

Despite the mounting need for change, online service providers have stalled the process, leaving children in a world of new technologies without adequate protections in place. As market giants, online service providers influence ongoing debates to limit legislative changes and the potential economic burden of those changes. Several scholarships have identified issues with the current system in the United States, but few have taken on the task of proposing a practical solution. To effectuate change, it is imperative to zero in on the most essential needs of children to adequately protect them online while balancing the concerns of those opposing large-scale modifications. This Note will begin by looking at the current law of child online privacy protections in the United States, COPPA, exploring how the act works, how violations are handled, and how the original version of COPPA has changed. Next, it will explore the approach recently taken by the United Kingdom and then evaluate how COPPA compares, as well as the discussions currently taking place regarding this topic. Lastly, this Note will set out a five-point plan to implement the necessary changes to bring children's online privacy protections into the 21st century.

---

* 2023 J.D. Candidate, University of Florida Levin College of Law. I would like to thank Professor Stacey Steinberg for being my faculty advisor and assisting me throughout this process. I would also like to thank my family, specifically my mother, Stacey Blanton, for encouraging me and assisting me throughout this journey. Lastly, I would like to thank Nadia Rossbach for always being a great friend and someone I could bounce ideas off. I could not have completed this work without the assistance of my friends, family, and mentors.

INTRODUCTION

Google was founded in 1998. Since then, there has been an array of innovative technologies, search engines, and social media developments, including Wikipedia in 2001, Facebook in 2004, YouTube in 2005, Twitter in 2006, the iPhone in 2008, and one of the most recent advancements to social media, TikTok in 2016.[1] These technological advancements over the last twenty-five years have been some of the most

1. Joshua Kim, *Technology Since 1998*, INSIDE HIGHER ED (Jan. 6, 2014), https://www.insidehighered.com/blogs/technology-and-learning/technology-1998 [https://perma.cc/T623-W8SE].

life-altering developments since the inception of the computer for both adults and children alike. However, since Google was founded, the United States has not implemented any new regulations for handling children's online privacy protections.[2] In fact, the most current updates since the creation of Google over two decades ago came about in 2012, marking another decade with minimal change.[3] This means that the decade-long gap since the last update to the regulations protecting children's online privacy goes back to before most of the children still considered protected under the regulation were born.[4]

The apparent negligence of the legislature and other involved parties is exactly what will be addressed in this Note, in addition to determining what advancements have been made in Great Britain and the changes that can be implemented now to ensure the online safety of our future generations. This Note will also explore why it has taken so long to change an obviously broken system and the efforts currently underway to help effectuate change in this area. Using social media platforms and other online service providers as a guide, the focus will be on exploring how to expand protections to include teenagers that are aged thirteen through seventeen. I will also examine other alternatives and resources for expanding the protection of children's online privacy rights by comparing the two policies at the forefront of these issues. The first is the current United States policy, the Children's Online Protection Policy Act (COPPA), and the second is the current policy in Great Britain, The Age-Appropriate Design Code (or the Children's Code), which was included in the 2018 Data Protection Act.[5] In this way, my analysis will shed light on the essential elements of the United States' policy in need of revision to bring the country into the 21st century with respect to online privacy protection for children.

---

2. *Id.*

3. *Id.*

4. The FTC issued a notice of proposed rulemaking to COPPA in 2011 and a supplemental notice of proposed rulemaking to COPPA in 2012. The FTC announced the publication of the amended rules to COPPA on December 19, 2012. Because of this the amendment is commonly referred to as the 2012 amendment to COPPA and will be referred to as such for the purpose of this Note. However, the amended rules to COPPA took effect starting on July 1, 2013. *See* Federal Trade Commission, *16 C.F.R. Part 312: Children's Online Privacy Protection Rule: Final Rule Amendments and Statement of Basis and Purpose* (Dec. 19, 2012), *available at* http://ftc.gov/os/2012/12/121219copp arulefrn.pdf [https://perma.cc/5D3K-8JJ8] (Final Rule and SBP); *see also* 16 C.F.R. § 312.

5. Byrin Romney, *Screens, Teens, and Porn Scenes: Legislative Approaches to Protecting Youth from Exposure to Pornography*, 45 VT. L. REV. 43, 45 (2020).

I. THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

COPPA was created in 1998 to help protect the personal information of children on the internet who are under the age of thirteen.[6] "COPPA applies to 'operators'[7] of commercial Web sites and certain other online services that are 'directed'[8] to children under thirteen."[9] The finding that an operator reaches children under the age of thirteen is not based on the actual express intent of the online service provider but rather on characteristics such as images or graphs used, the language used to reach individuals, and the presentation of the website as a whole.[10] Even if the service providers are not directing their attention specifically toward reaching children under the age of thirteen, as long as there is actual knowledge that providers are collecting personal information[11] from these children, then the online provider will still fall under COPPA.

---

6. 16 C.F.R. § 312.2.

7. After the 2012 amendment to COPPA, operator

> means any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that Web site or online service, where such Web site or online service is operated for commercial purposes involving commerce among the several States or with 1 or more foreign nations; in any territory of the United States or in the District of Columbia, or between any such territory and another such territory or any State or foreign nation; or between the District of Columbia and any State, territory, or foreign nation.

Id.

8. As long as an operator knowingly collects information from children in the United States then they are bound by COPPA. Even if a web-based operator is a foreign entity and they intend to reach children under the age of thirteen in the United States, they still fall under the parameters of COPPA. Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751, 760 (2001).

9. *Id.* Many questions arise as to why the cutoff age is thirteen when there are so many other programs, like FERPA, where parents can still access the school record of a child under the age of eighteen even if the teen objects. *Id.* at 759. The reasoning given by the FTC is limited, "that the age of thirteen is the standard for distinguishing adolescents from young children who may need special protections." *Id.* Nevertheless, the FTC fails to explain why it would assume that children between the ages of thirteen and seventeen do not need such protection and also that those children would fully understand the negative ramifications of revealing private personal information to operators of online services. *Id.*

10. *Id.* at 760–61.

11. Personal information in the eyes of COPPA "is defined broadly to include a person's name, address, e-mail address, phone number, social security number, and any other identifier deemed to enable physical or online contact." Allen, *supra* note 8, at 761.

A. *The Requirements for Online Service Providers*

COPPA has five requirements that must be met in order to comply with the regulation: notice, verifiable parental consent, parental review, security, and limits on the use of games and prizes.[12] To fully understand what COPPA truly entails, it is important to break down each component individually. To start, online service providers must provide notice to the parents of children who want to access the websites that collect information about users before any of the children's information is collected.[13] The notice requirement must provide parents with the following information:

> (1) "a description of the specific types of personal information collected from the child by [the] operator"; (2) "the opportunity at any time to refuse to permit the operator's further use or maintenance . . . of personal information from that child"; and (3) "a means that is reasonable . . . for the parent to obtain any personal information collected from that child."[14]

Further, this information "must be within the four corners of the notice . . . [c]ompanies must also send this notice directly to the parent and must post a prominent and clearly labeled link to an online notice of its information practices . . . ."[15] This is important because it allows parents to continuously regulate what type of information a site obtains so that even if certain personal information is revealed by the child without the parent's knowledge, the parent can attempt to have the information removed.[16]

The parental consent and review requirement involves gaining the consent of the parent in a verifiable way and giving the parent a reasonable avenue for reviewing the personal information collected on the child.[17] COPPA does not specifically outline a defined mechanism for obtaining this consent.[18] Therefore, "[t]he operator of a Web site may obtain parental consent online and verify that consent via e-mail or

---

12. Tianna Gadbaw, *Legislative Update: Children's Online Privacy Protection Act of 1998*, 36 CHILDREN'S LEG. RIGHTS J. 228, 228 (2016).

13. Gianna Korpita, *It's a Small World After All: How Disney's Targeted Advertisements Implicate COPPA*, 19 J. HIGH TECH. L. 407, 414–15 (2019).

14. Allen, *supra* note 8, at 763.

15. Korpita, *supra* note 13, at 417.

16. *See Complying with COPPA: Frequently Asked Questions*, FTC (July 2020), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions [https://perma.cc/Q2KX-BRRS].

17. 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, 831 (2020).

18. Allen, *supra* note 8, at 761.

telephone if the personal information is used only internally."[19] There are certain exceptions to the requirement of parental consent.[20] For one, an online service provider can gather personal information if it is used "to protect the safety of children, the security of the site, and to satisfy the demands of law enforcement."[21] Operators may also, on a one-time basis, collect only email addresses from a child in order to process the request as long as such information is properly deleted afterward.[22] Another important point of distinction is that COPPA only regulates commercial sites. If such sites are not considered commercial for the purpose of COPPA, they are not restricted.[23]

For purposes of the security requirement, the language of the regulation states that "[a]n operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete[24] all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records. . . ."[25]

COPPA also states that operators must use "reasonable security" measures to protect personal information.[26] However, neither the Federal Trade Commission (FTC) nor the statute specifically define what this entails.[27] Instead, operators are left with the suggestion "to minimize the amount of data collected from children, retain this data for as short a period as possible, and make certain that any third parties who access this data maintain strong security."[28] Consequently, the guidelines leave loopholes for operators and allow them to make their own rules when it comes to the reasonable security requirement under COPPA.[29]

The last requirement is the limit on the use of games and prizes.[30] This limitation consists of prohibiting operators from using incentives that lead to a large influx of private and personal information from the children who play such games due to the appeal these incentives have on influencing the child's decision to take part in the activity.[31] In other

19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.* at 762.
24. "Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business." 16 C.F.R. § 312.2.
25. *Id.*
26. Jeremy Greenberg, *Dangerous Games: Connected Toys, COPPA, and Bad Security*, 2 GEO. L. TECH. REV. 170, 176 (2017).
27. *Id.*
28. *Id.*
29. *Id.*
30. Emily DiRoma, *Kids Say the Darndest Things: Minors and the Internet*, 2019 CARDOZO L. REV. DE NOVO 43, 53 (2019).
31. *Id.* at 46.

words, the limitations on the use of games and prizes provide that operators can only acquire personal information that "is reasonably necessary to participate in the activity."[32] Again, this allows operators to determine what is reasonable in terms of the information they acquire relative to the use of games and prizes.

B. *The Interworking of COPPA and How Violations Are Addressed*

COPPA allows the FTC to act against violators of COPPA,[33] specifically the "operators" of websites and other online services.[34] However, a preemption provision in COPPA restricts private parties from filing a claim under statutes pertaining to state consumer protection.[35] Further, COPPA explicitly states that "[n]o State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in [this regulation] that is inconsistent with the treatment of those activities or actions under this section."[36] In other words, state and local governments cannot bring action against online service providers under state consumer protection laws.[37]

In addition, COPPA limits the Attorney General from producing claims that fall under state consumer protection laws, or the equivalent, that interfere with COPPA.[38] Different courts have interpreted this provision in different ways.[39] For example, the Courts of Appeal for the Third Circuit determined that a claim could be brought as long as the operator was deceptive in how the children's information was acquired "as to create a false expectation of privacy."[40] However, COPPA allows the Attorney General "to bring suit to enjoin practices in violation of the statute, enforce compliance, obtain damage, restitution or other compensation on behalf of residents of the applicable state, or obtain other such relief as a court may deem appropriate."[41] Therefore, it is possible for the Attorney General to bring legal action against the operators under certain limited circumstances.[42]

Ultimately, legal action regarding children's online privacy is taken at the federal level, primarily through the Federal Trade Commission.[43]

---

32. Allen, *supra* note 8, at 764.
33. 16 C.F.R. § 312.2.
34. 1 Robert Brownstone & Tyler Newby, *Data Sec. & Privacy Law* § 9:89 (2022–2023).
35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.*
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.*
43. *Id.*

Unfortunately, the reality is that it took the FTC three years to bring any action after the COPPA amendments were codified in 2013, and the Attorneys General rarely, if ever, use their power to bring claims against operators.[44]

C. *The 2012 Amendments to the Children's Online Privacy Protection Act*

Until December 2012, online privacy protections for children were handled through the 1998 version of COPPA. However, in 2012, the FTC amended COPPA due to the expansive development of technology in the new century.[45] With the intent of creating impactful changes to the way we handle children's online privacy, the modifications served only to resolve ambiguities from the 1998 version, along with a few other minor updates.[46] For example, the 2012 version redefined operators,[47] websites, and/or online services directed toward children and personal information.[48] The change in the definition of personal information has provided "parents additional control over the collection of their children's data."[49]

The 2012 changes also kept children's online information more secure.[50] The 2012 amendment to COPPA limits operators from keeping personal information of children "only as long as reasonably necessary."[51] When an operator decides the information is no longer needed, operators have the duty to use reasonable measures to protect the information from unauthorized access.[52] This is different from the 1998 version of COPPA, where operators were not instructed to discard information when no longer needed, but rather, they were left to decide what to do with the information. Furthermore, the new law clarified that operators must take "reasonable steps to release personal information

44. *Id.*

45. Gadbaw, *supra* note 12, at 229.

46. *Id.*

47. In the 2012 amendment, Operator includes any "operator of a child-directed site or service where it allows outside services to collect personal information from its visitors." This allowed an ongoing issue to be resolved where third parties were collecting the personal information of children on behalf of the online service providers. *Id.*

48. In the 2012 amendment, personal information "was re-defined to include 'geological information as well as photos, videos, and audio files of a child's image or voice.'" This allowed physical information to be protected as well. *Id.*

49. Diana S. Skowronski, *COPPA and Educational Technologies: The Need for Additional Online Privacy Protections for Students*, 38 GA. ST. U. L. REV. 1219, 1230 (2022).

50. Gadbaw, *supra* note 12, at 229.

51. *Id.*

52. *Id.* at 229–30.

only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of such information."[53]

Another noteworthy improvement relates to the use of "safe harbor programs."[54] Online service providers who wish to take advantage of safe harbor provisions are now required to "conduct annual comprehensive reviews of their member's information practices and submit to the FTC annual reports of the results of these annual reviews."[55] Further, the 2012 revisions gave service providers other ways of acquiring parental consent.[56] For instance, it is now permissible for companies to acquire parental approval "through electronic scans of signed parental consent forms, videoconferencing, use of government-issued ID, and alternative payment systems."[57] Operators can also attain approval by adhering to "a 120-day notice and comment process conducted by the FTC."[58] With these new methods, companies can match faces to different forms of personal identification of the parents to acquire the consent needed.[59] The amendments to the 1998 version of COPPA have helped to make impactful changes to children's online privacy. Since then, the United States has fallen behind in comparison to other countries, like the United Kingdom, that have made substantial changes to keep up to date with the growing number of technological advances.

II. THE UNITED KINGDOM POLICIES ON CHILDREN'S ONLINE PRIVACY: THE AGE-APPROPRIATE DESIGN CODE (THE CHILDREN'S CODE)

Due to the growing number of children being exposed to the internet, the need for increased protection for children's online privacy rights has sparked action in the United Kingdom. The United Kingdom has become aware of the use of data collection by online service providers and the fact that the collection process begins once an individual downloads an application and commences to play or use the app.[60] They also recognized

53. *Id.* at 230. *See also* David R. Hostetler & Seiko F. Okada, *Children's Privacy in Virtual K-12 Education: Virtual Solutions of the Amended Children's Online Privacy Protection Act (COPPA) Rule*, 14 N.C.J.L. & TECH. ONLINE 167, 168 (2013) (stating that the 2012 amendment "strengthens regulation over website operators and by expanding COPPA's reach to mobile application developers and third-party vendors . . . .").

54. Under the 1998 version of COPPA, "the safe harbor provision encouraged industry self-regulation by allowing approved industry members to create their own COPPA oversight programs with their own compliance guidelines." Gadbaw, *supra* note 12, at 230. Furthermore, "[w]ebsite operators who participated in these approved safe harbor programs were subject only to the provisions of their own self-created and self-regulated safe harbor program in lieu of FTC enforcement." *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

60. INFORMATION COMMISSIONER'S OFFICE, AGE APPROPRIATE DESIGN: A CODE OF

that one out of five users is a child.[61] Further, the amount of time all humans currently spend using services from online providers has grown exponentially.[62] The upsurge in time spent using these services has also augmented how this type of content is shaping the lives of everyone, especially children.[63] Without certain safeguards in place to protect them, the risk of harmful consequences is higher than ever.[64] Thus, the United Kingdom enacted the Age-Appropriate Design Code, or the Children's Code, becoming a force of law on September 2, 2020.[65]

The Children's Code outlines fifteen standards that companies must follow, keeping the child's best interest at the forefront.[66] The Code applies to all online service providers likely to be accessed by children in the country, which the United Kingdom calls information society services (ISS).[67] If a company is found not adhering to the guidelines of the Children's Code, the company would be in violation of the Privacy and Electronic Communication Regulation (PECR) and the General Data Protection Regulation (GDPR).[68] As a consequence of the violation, action may be taken against the company or organization, including "assessment notices, warnings, reprimands, enforcement notices, and penalty notices . . . . For serious breaches of the data protection principles, [the agencies] have the power to issue fines of up to €20 million . . . or 4% of [a company's] annual worldwide turnover, whichever is higher."[69] This can result in a hefty penalty for those who do not obey the standards; however, violators are often given a chance to rectify the issues associated with the violation.[70]

The Children's Code's specific standards include the children's best interest, data protection impact assessments, age-appropriate application, detrimental use of data, default settings, geolocation, parental controls, and online tools.[71] Children's best interest comes from the United Nations Convention on the Rights of Children (UNCRC).[72] Article Three of the Convention states that "[i]n all actions concerning children, whether

---

PRACTICE FOR ONLINE SERVICES, 9 (Sept. 2, 2020).

61. *Id.* at 3.

62. *Id.*

63. *Id.*

64. *Id.* at 30.

65. *Id.* at 32.

66. *Id.* at 7–8

67. "The definition of an ISS is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.'" This encompasses most for-profit online services and even includes electronic services for controlling connected toys and other devices. *Id.* at 16.

68. *Id.* at 5.

69. *Id.* at 12.

70. *Id.*

71. *Id.* at 7–8.

72. *Id.* at 24.

undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."[73] Indeed, one of the main goals of this new regulation is to allow children more access to the Internet, which includes more access to information, more opportunities to interact with others, and more ways to further the promotion of their development through various forms of technology and games.[74] Further, relying on the best interest standard, the United Kingdom asserts that children should have the right to privacy and freedom from companies' economic exploitation.[75] The Code also incorporates another important standard: the detrimental use of data.[76] This standard is in place to ensure a child's personal data is not used in such a way that has been shown to be detrimental to the well-being of the child.[77] It also ensures that providers' policies do not contradict industry or government-set standards.[78]

Next, the data protection impact assessments (DPIA) standard is a seven-step assessment[79] with goals to "help you identify and minimize the data protection risks of your service—and in particular, the specific risks to children who are likely to access your service which arises from your processing of their personal data."[80] Under the GDPR, this type of assessment is required before starting any "type of processing that is likely to result in a high risk to the rights and freedoms of individuals."[81] One of the more important aspects of this seven-step process is the consultation with parents and children, which requires a hands-on approach to reviewing the risks to privacy associated with certain company protocols and conducting research from consumers of the online service to ensure they are aware of how personal information is being used.[82] This hands-on approach is instrumental in allowing operators to see exactly what kinds of activities are occurring within the companies regarding the collection of children's data.

The age-appropriate application is one of the most important standards in the Children's Code and one that other countries, including

---

73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.* at 43.
77. *Id.* at 43–44.
78. *Id.* at 43.
79. The seven-step program includes: "identify[ing] the need for a DPIA; describe[ing] the processing; consider[ing] consultation; assess[ing] necessity and proportionality; identify[ing] and assess[ing] risks arising from your processing; identify[ing] measures to mitigate the risks; sign[ing] off, record[ing] and integrat[ing] outcomes. Importantly, the process was created to be a more flexible and scalable system." *Id.* at 27.
80. *Id.*
81. *Id.*
82. *Id.* at 28.

the United States, should implement to move into the 21st century where children's online privacy protection is concerned.[83] The application assesses the different needs of children based on each child's age level and stage of development.[84] Using this type of information, children are afforded the appropriate level of protection by allowing for flexibility in determining the proper standards based on the online services children are actually using.[85] Additionally, the Code gives online service providers a standard for all users so they do not have to assess what age bucket a child fits into that could potentially require a different form of protection.[86]

The delineated age periods include zero to five or pre-literate and early literacy, six to nine or core primary school years, ten to twelve or transition years, thirteen to fifteen or early teens, and sixteen to seventeen or approaching adulthood.[87] However, it is important to note these are not the required age ranges or classifications but rather a guide as to what age groups may need a different protection category.[88] This concept also allows the online service provider to use any method necessary to determine a user's age as long as the information is obtained accurately.[89] A few methods to determine the user's age include self-declaration, artificial intelligence, third-party verification services, account holder confirmation, technical measures, and hard identifiers such as formal documents, like a passport.[90] However, as innovative and creative as these methods may be, online service providers have been reluctant to implement these methods due to the additional cost and time.

The next standards are the default settings and geolocation, which highlight the idea that the use of certain settings ensures online privacy protection.[91] This means setting a "high privacy" standard as a default unless a company can provide a compelling reason why the standard should be different.[92] Likewise, for geolocation, the standard of the Children's Code is for those settings to be turned off in order to protect the child's location.[93] The default settings are simple aspects of the standards that can profoundly affect ensuring children are protected from inadvertently oversharing personal information by simply using the tools within the provider's application or program.

---

83. *Id.* at 32.
84. *Id.*
85. *Id.*
86. *Id.* at 32–33.
87. *Id.*
88. *Id.* at 32.
89. *Id.* at 33.
90. *Id.* at 34.
91. *Id.* at 5.
92. *Id.* at 7.
93. *Id.*

Parental controls provide another layer of protection within the arsenal of standards while also ensuring children can freely express themselves on the internet.[94] These types of controls provide age-appropriate information to children regarding how the parents monitor their use of certain applications.[95] The idea is that, depending on the child's age, if a parent is given access to monitor the child's activity or track their location, he/she should be made aware that a parent is monitoring them.[96]

The final standard involves the use of online tools to ensure that children have the proper resources needed so they are able to exercise their data protection rights and report any concerns regarding their personal information.[97] These standards can be used by other countries, especially the United States, as a guideline to understanding the methods and ideas implemented in other areas that could be helpful in making impactful changes to how children's online privacy is treated.[98]

III. TIME FOR CHANGE: THE CURRENT DEBATE ON REVISIONS TO COPPA AND WHAT IS CURRENTLY BEING DONE

A lot of the changes that have been implemented around the world, like the Children's Code in the United Kingdom, have not been passed free from debate. After all, there is a reason the last change to COPPA was over ten years ago, despite the growing number of technological advancements. Both sides of the debate have valid reasons and viewpoints as to why certain changes to COPPA should or should not be implemented. To truly advocate for substantive change to COPPA, both sides must be discussed, and the arguments for and against should be fleshed out.

A. *Potential Downsides of Revision to COPPA and What Can Be Done to Counter the Issues*

One issue that commonly emerges is the idea that, given the current restrictions of COPPA, children have been removed from certain online platforms, impairing their ability to freely express themselves on the internet, especially children under the age of thirteen who are currently affected by COPPA.[99] Often, online service providers take the easy and sometimes cheaper way out when adhering to the regulations of COPPA

94. *Id.*
95. *Id.* at 10.
96. *Id.* at 40.
97. *Id.* at 8.
98. *Id.* at 3.
99. Sasha Grandison, *The Child Online Privacy Protection Act: The Relationship Between Constitutional Rights and the Protection of Children*, 14 U. D.C. L. REV. 209, 219 (2011).

by simply banning use by children under the age of thirteen.[100] These online service providers recognize that they will be able to withstand the "missed opportunity" of not allowing children under the age of thirteen to join because children are not easily thwarted by a simple age verification screen.[101] In other words, children simply lie about their age to circumvent this barrier.[102] As a result, children are now truly unprotected when it comes to these sites acquiring their private information, similar to the circumstances going back to the mid-nineties before there was any protection.[103]

Individuals and groups opposed to revisions to COPPA raise concerns that extra regulations will further hinder the ability of youth to access the internet and freely express themselves without government intervention.[104] This concept may seem reasonable to outsiders who are not familiar with COPPA and other protections that have been executed globally, but to those who truly understand what increased privacy protection for children will do, this is not the case at all. In fact, it will do exactly the opposite.[105] The practical effect of regulation around online privacy is not to stop children from participating online or using the applications of online service providers. Instead, it allows children to play and interact freely on the internet without fear, or even worse, the lack of fear due to ignorance.[106]

Another critique of COPPA and any further revision is the idea that an increase in restrictions that cause companies to implement safeguards creates an economic burden.[107] Thus, small businesses, specifically those in the midst of growth, are now affected at the front end and unable to afford the cost of putting proper protections in place as required by law.[108] This can inadvertently lead to online service powerhouses that control a majority of the market, stifling startup companies and essentially creating a monopoly of large companies that control everything.[109] This includes the power to force and push through legislation that will allow these powerhouses to gain even more strength in their respective markets and

100. DiRoma, *supra* note 30, at 61.

101. *Id.*

102. *Id.*

103. *Id.*

104. EY UK Privacy and Data Governance Channel, *Protecting Children Online: The Age Appropriate Design Code*, at 18:23 (Nov. 16, 2021), (downloaded using Spotify) https://open.spotify.com/episode/5t9AVgXhaQ2FCdrwe34NAl?si=Zfxqu5JJRQKqj1MPdE3PKQ [https://perma.cc/9S8X-GR9D].

105. *Id.* at 06:30.

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

to further absolve them of their responsibility to protect the online privacy of our youth.[110]

To illustrate, the Children's Code in the United Kingdom has implemented more restrictions and heightened regulatory requirements that online service providers must follow to comply with the new laws.[111] The commonly mentioned concern with the Children's Code is related to the same issue of stifling development and impeding small businesses from flourishing.[112] This is a valid concern because the law involves increased regulatory requirements and a push for an age-appropriate standard, increasing operator costs.[113] Still, this issue can be absolved by using the different resources the United Kingdom has made available to assist with these problems.[114] One such resource is a technical standard published by the British Standards Institute, created for the purpose of training companies on how to perform an identity attribute check to verify a user's age.[115]

The standard verifies an assertion of parental responsibility in a way that does not violate children's privacy and still adheres to the requirements of the Children's Code by only collecting data on a temporary basis.[116] Companies are wary of the technical implications of the standard.[117] However, the technical aspect is mostly API integrations,[118] which are common in credit reference agencies, so this is not a new notion.[119] It should be noted that "[n]o matter the business and the size of the enterprise, APIs enable seamless operation and performance of applications and web systems."[120] Additionally, the models and procedures in the published guides by the British Standards Institute have suggestions regarding methods that can be used to implement the new regulations.[121] It can be used over and over in a

110. *Id.*

111. INFORMATION COMMISSIONER'S OFFICE, *supra* note 60, at 11.

112. DiRoma, *supra* note 30, at 61.

113. EY UK Privacy and Data Governance Channel, *supra* note 104, at 08:26.

114. *Id.* at 08:35.

115. *Id.*

116. *Id.* at 08:38.

117. *Id.*

118. API integrations can be described as "the connection between two or more applications via their APIs (application programming interfaces) that allow systems to exchange data sources. API integrations power processes throughout many sectors and layers of an organization to keep data in sync, enhance productivity and drive revenue." Thomas Jones, *What is an API Integration? (A guide for non-technical people)*, GENERATION DIGIT. (May 11, 2021), https://www.gend.co/blog/what-is-api-integration-a-guide-for-non-technical-people[https://perma.cc/TRT6-XEVY].

119. EY UK Privacy and Data Governance Channel, *supra* note 104, at 09:10.

120. Jones, *supra* note 118.

121. *Id.*

formalistic process that is a zero data and knowledge model[122] to protect children and parental information.[123]

Lastly, the chief question typically posed relates to the cost of acquiring the information and the burden of implementing the process for smaller companies that are just starting out, but under the United Kingdom's system, these resources are provided at no cost.[124] Therefore, if a common model or procedure could be employed at the same time as a revision to COPPA, it could provide resources for smaller companies, and the issue would be greatly diminished.[125] Also, it should be noted that the model published by the British Standards Institute is a globally used model.[126]

B. *What Is Currently Being Done in the Area of Children's Online Privacy Protection in the United States*

There are several groups around the country that are working to revise and update the much-outdated system that is COPPA.[127] These groups are comprised of individuals with various degrees of interest, including concerned parents advocating for change, state governments and legislatures that are working to make a difference within their own borders, as well as federal legislatures that are vying for support on bills that can generate change directly to the current law.[128] An examination of these projects is the best way to understand what local and state governments have been doing and what matters are being pushed to their legislatures to create impactful changes in child privacy rights.[129]

There are currently three bills being considered that would expand online protection for children; however, none have gained enough support to revise COPPA, and only two are worth mentioning for this Note.[130] The third bill, the Eliminating Abusive Rampant Neglect of Interactive Technologies or EARN IT Act, is directed toward the

122. Zero data and knowledge model means that this procedure can be completed without taking any data or information of the potential user or the parent of the potential user, so no information or data is obtained by running this age verification check. EY UK Privacy and Data Governance Channel, *supra* note 104, at 09:24.

123. *Id.*

124. *Id.* at 09:48.

125. *Id.*

126. *Id.* at 08:53.

127. Electronic Privacy Information Center, *Children's Privacy*, EPIC.ORG (last visited Feb. 21, 2023), https://epic.org/issues/data-protection/childrens-privacy/ [https://perma.cc/S6AL-9NUC].

128. *Id.*

129. Michael P. Canty, Carol C. Villegas, & Danielle Izzo, *Assessing 3 Bills To Expand Kids' Online Protections In 2022*, LABATON SUCHAROW (Feb. 4, 2022), https://www.labaton.com/blog/assessing-3-bills-to-expand-kids-online-protections-in-2022 [https://perma.cc/S78F-GLKK].

130. *Id.*

insulation of online service providers and directly relates to specific instances of child exploitation that are beyond the scope of this Note.[131]

The first bill worth mentioning is a proposed amendment to COPPA, which includes changing the cutoff age from thirteen to fifteen; lowering the standard for knowledge from actual knowledge to constructive knowledge; forbidding advertising that targets minors; providing a feature that will allow minors the opportunity to delete any personal information obtained by online providers; forcing obligations for online providers to label detailed disclosures in regard to the information obtained; creating a program within the FTC to regulate online marketing directed at minors.[132] The second is a new act called the Kids Internet Design and Safety, or KIDS.[133] The major components of this act include changing the age threshold for protection to sixteen, similar to the previous idea; lowering the standard to constructive knowledge; prohibiting particular interfaces or functional components that target children; limiting the scope of algorithms; increasing guidelines and prohibiting certain explicit content from reaching children.[134]

Both proposals are very forward-thinking and would help resolve several issues relative to the current system. Yet what they seem to lack are more details and resources that can be implemented to create substantive change. For instance, limiting the scope of algorithms is a great tool for keeping service providers from acquiring personal information from young users to develop marketing and advertising focused directly on the specific wants of children. However, the lack of specific guidelines provided to service providers regarding what they can and cannot do and the lack of resources to help the providers adhere to these guidelines is problematic. Essentially, the providers are largely left unregulated because the FTC and others like them fail to keep up to date on current business systems and technologies and knowledge of current issues children face online. If the FTC neglects to provide the proper resources to manage the additional requirements, the cycle of having regulations in place without proper enforcement will continue to render all the changes considered ineffective. However, with the proper resources and enforcement in place, one can ensure that service providers can continue to do business efficiently while simultaneously protecting the interest of children's privacy rights.

131. *Id.*
132. *Id.*
133. *Id.*
134. *Id.*

IV. MEETING THE NEEDS OF THE 21ST CENTURY: A FIVE-POINT PLAN FOR REVISING COPPA

As emphasized throughout this Note, the amount of time that has passed since changes to COPPA were last made is astounding. Consequently, both advocates and critics of COPPA tend to agree that some type of change is in order; however, what exactly should be done is the more challenging question. To garner the necessary support for legislative reform, it is critical to balance protecting children's interests online and enacting changes that service providers can easily implement. Therefore, one must determine the most critical issues currently endangering children's online privacy and provide only the most essential safeguards for their protection. As such, I have laid out a five-point plan of the most significant revisions that need to be implemented to create a lasting impact on children's online privacy rights.

A. *Expansion of Protections to the Ages of Thirteen to Seventeen*

First, one of the most imperative changes for COPPA to be as effective as possible is the expansion of protection to cover children from ages thirteen to seventeen. The increase in age protection was discussed in the two bills currently being debated by Congress and was also mentioned in the United Kingdom's Age-Appropriate Design Code.[135] Importantly, "[t]eenagers ages thirteen to seventeen are going online increasingly more frequently than ever before. A recent study by the Pew Research Center found that ninety-two percent of teenagers report going online daily--including twenty-four percent who say they go online almost constantly."[136] As such, those who need online privacy protection the most are, in fact, children between the ages of thirteen and seventeen.

A common argument against expanding protection to children in this upper age bracket is that they have enough life experience or knowledge to be properly protected without outside intervention. However, this is often not the case.[137] These groups include individuals beginning to transition into high school, beginning to drive, and actively and independently participating as consumers in the market for the first time. As a result, a number of these individuals step into a vulnerable position of acquiring a new form of freedom while lacking a complete

135. Canty, Villegas, & Izzo, *supra* note 129; *See also* INFORMATION COMMISSIONER'S OFFICE, *supra* note 60.

136. DiRoma, *supra* note 30, at 47.

137. Indeed, other areas of the law seem to agree with the notion that children of this age range require extra protection. First, "[t]eens are still legally defined as minors and cannot legally enter into binding contracts--including privacy policies frequently found on the Internet." *See id.* at 61. Moreover, under FERPA, a child under the age of eighteen cannot prevent her parents from accessing her school records nor can a child override a parent's veto of her school record disclosure if the record is sought by the child. Allen, *supra* note 8, at 759.

understanding of the possible ramifications of their actions. Indeed, "California's legislature concluded that children and teenagers, compared to their adult counterparts, were at greater risk online because they lack fully developed self-regulating abilities and easily succumb to online-driven peer pressure."[138]

For instance, "[h]igh social media use can lead minors to [be] inundated with numerous advertisements and products. Simply by logging into a social media site, internet users of all ages are exposed to advertisements on a wide range of services from clothing stores to restaurants to the newest indoor tanning locations."[139] Most troubling, online-directed advertisements and marketing promotions often expose children in this age bracket to products that can be sexually explicit or related to the tobacco or vaping industries.[140] These industries are mindful that starting children off at an early age can enhance the possibility of addiction and continued use of their product.[141] Their unregulated advertisements directed toward older children boost the peer pressure already prevalent in a teenager's daily life.[142] Ultimately, the vulnerabilities of older children also require online privacy protection to prevent service providers from exploiting personal information to market certain products to these children coercively.

B. *Age-Appropriate Design*

Next, some form of the United Kingdom's age-appropriate design should be implemented.[143] Specifically, initiating a different set of protections based on the ages of the children involved, as done in the United Kingdom, would be invaluable to children's online privacy.[144] To effectuate this change, online service providers should complete DPIAs, and the information collected should be turned over to the appropriate governmental agencies.[145] These agencies will then use the information to create guidelines based on a child's age. This will ensure that safeguards and standards are properly constructed based on the age of users.

The individualized protection would resolve much of the debate surrounding the issue of expanding COPPA protections to those under eighteen. The age-specific structuring of the system would expand protection while recognizing a seventeen-year-old's protection needs are

138. DiRoma, *supra* note 30, at 57.
139. *Id.*
140. *Id.* at 45
141. *Id.* at 48.
142. *Id.*
143. INFORMATION COMMISSIONER'S OFFICE, *supra* note 60, at 23.
144. *Id.* at 32.
145. *Id.* at 27–31.

uniquely different from the protections needed for a seven-year-old. Children have different capacities of understanding and behaviors at different ages. Therefore, an arrangement in place that does not allow latitude in conjunction with a child's developmental stage may impose far too much protection on some and far too little on others. As noted previously, child privacy standards should not be addressed with an all-or-nothing approach, but rather, the standards should be structured for a child's particular online use in a way that will meet their needs as they develop.[146]

An individualized approach to child privacy also helps alleviate some of the concerns commonly debated regarding the restriction of a child's free access to the use of the internet. Protections tailored toward a specific age range will not restrict a child's ability to access the internet freely because children tend to use it according to their developmental stage. Any protection, in this case, would be implemented precisely to make up for a specific lack of capacity a child may have based on his or her age.

C. *Right to Have Personal Information Deleted*

The third part of the plan is the ability for children, or the parents of children, to request that certain private information be deleted.[147] This goes hand in hand with the concept of the "right to be forgotten."[148] In essence, depending on the child's age, a child, or his parents should be able to remove personal information on the internet, which is deemed detrimental.[149]

Contrary to the notion that "[g]rowing up is synonymous with learning from one's mistakes and teenagers deserve the chance to erase their foolish mistakes in private, *without the threat of future repercussions from future onlookers*,"[150] there is no current right to remove personal

146. *Id.* at 32–33.

147. This is a highly debated topic due to the effect it could have on the First Amendment's freedom of the press. *See* Amy Gajda, *Privacy, Press, and the Right to Be Forgotten in the United States*, 93 WASH. L. REV. 201, 203 (2018). However, the narrow classification of private personal information disclosed only to online service providers for age verification, or a similar purpose, should not offend the First Amendment, as it is not information that an individual voluntarily and under no pressure from an additional source decided to post or reveal. Instead, it is personal information required to be provided for an individual to use the online provider's service that is then used for advertising and other purposes. Additionally, the personal information acquired by providers is often not of the nature that can be viewed as furthering any new product or storyline that the public has the right to access, but rather it is used by providers to increase revenue and trick young users into marketing ploys.

148. Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 89 (2012); *see also* Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839, 864 (2017).

149. *See* Ashley Stenning, *Gone but Not Forgotten: Recognizing the Right to Be Forgotten in the U.S. to Lessen the Impacts of Data Breaches*, 18 S.D. INTL. L.J. 129, 132 (2016).

150. DiRoma, *supra* note 30, at 65 (emphasis added).

information once it exists in the online world. A minor's online image can drastically affect her life, as that minor will eventually enter the working world or attend college, and how these individuals are portrayed on social media is a common way for employers or admissions personnel to assess an individual. In fact, "[s]chools and employers are rejecting young people for school programs, internships, college admissions, and jobs after researching applicants' online activities and posts."[151] Therefore, the ability of children to request their information be deleted is a fundamental concept and one of grave importance in children's online protection.

D. *Default Settings*

Another part of the plan is the implementation of certain default settings. Children, and even parents, are not always aware of exactly how and what information is being obtained, which can leave children vulnerable by default.[152] Thus, the required default settings should be that of high privacy protection rather than defaulting to little or no protection. The whole idea of increasing protections is because children do not have the capacity to understand what safeguards they need to protect their information.[153] Therefore, having the privacy protections default on the higher end makes sense.

As mentioned previously, a common argument against using default settings as a means of data protection is the presumption that parents help decide on and implement certain settings.[154] However, the unfortunate reality is that not all parents are involved in the process the way one might think.[155] Children often have parents who do not understand the complexities of the internet, parents who are too busy working and handling other tasks to implement the proper protections or even parents who have no knowledge that their child is using an application that is acquiring personal information.[156] Furthermore, "[p]arents find it difficult to restrict access because children are often savvier than their parents at finding and accessing Internet materials."[157] As a result,

151. *Id.* at 49.

152. Susan G. Archambault, *Student Privacy in the Digital Age*, 2021 B.Y.U. EDUC. & L.J. 1, 8 (2021).

153. *Id.*

154. Melanie L. Hersh, *Is COPPA A Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children's Interests on the Internet*, 28 FORDHAM URB. L.J. 1831, 1835–36 (2001).

155. Brooke Auxier, Monica Anderson, Andrew Perrin & Erica Turner, *Parents' Attitudes – and Experiences – Related to Digital Technology*, PEW RSCH. CTR. (July 28, 2020), https://www.pewresearch.org/internet/2020/07/28/parents-attitudes-and-experiences-related-to-digital-technology/ [https://perma.cc/M5G3-ZYAG].

156. *Id.*

157. Hersh, *supra* note 154, at 1832.

children often use the internet with no or very little parental restriction or supervision.

Additionally, the government is the one best situated to understand what is affecting our children online and the nuances that cover this growing topic.[158] In fact, "it has been held that both parents and the government have a legal basis for protecting children."[159] Governmental agencies, specifically the FTC, are the intermediaries between online service providers, children, and parents. As such, they are the ones getting up-to-date information on violations to COPPA and what is happening in the real world in relation to this issue. Therefore, the government should be the one to apply and regulate these default settings to ensure children are protected while having the parents as an additional safeguard. In the end, ensuring adequate default settings are in place as frontline protection will result in a step in the right direction for protecting children's private information online, and together with the last part of the plan, will serve to maximize that protection.

E. *Best Interest of the Child*

The last part of the five-point plan is to require that online service providers and all players involved in the process always account for the child's best interest. At first, it may seem to be an ambiguous provision to include, but it is vital to the success of the entire plan. The essence of this provision serves its purpose whenever any ambiguity arises or when an online service provider is unclear about what action should be taken. At that point, the provider should follow the guideline that works in the child's best interest. This should always prevail, no matter the situation. All the plan components work together to increase protection and ensure that every child under eighteen has the proper safeguards; however, without constant reminders, children can be forgotten or overlooked. As mentioned previously, this is not a new idea created by the United Kingdom when crafting the Age-Appropriate Design Code; instead, it is an idea grounded in basic human rights and coined by the United Nations.[160] Online providers must recognize the importance of this protection and make it a part of their daily tasks to keep the interest of the children at the forefront of their operations.

158. *Id.* at 1859.

159. *Id.* at 1835.

160. INFORMATION COMMISSIONER'S OFFICE, *supra* note 60, at 3.

CONCLUSION

As technology and the manner in which children interact on the internet change, the law, too, must change. Technology is advancing at too great a rate for children's online privacy protection to be stuck in the late 20th century. The plan proposed in this Note incorporates only a fraction of amendments that may be implemented to protect our youth better. However, it is an essential first step to creating substantive change. Implementing a practical solution will help alleviate stress and overcome the greatest hurdle preventing the law from developing alongside technology—the economic and administrability burden imposed on online service providers. Ultimately, children today are being exposed to risky circumstances, and it is our responsibility as parents, online service providers, and even young adults who were recently in the same predicament to step up and push for lasting change that will bring children's online privacy rights into the 21st century while simultaneously protecting the innocence of our youth.