Georgia State University Law Review

Volume 38
Issue 4 *Summer 2022*

Article 12

6-1-2022

COPPA and Educational Technologies: The Need for Additional Online Privacy Protections for Students

Diana S. Skowronski
dskowronski1@student.gsu.edu

COPPA AND EDUCATIONAL TECHNOLOGIES: THE NEED FOR ADDITIONAL ONLINE PRIVACY PROTECTIONS FOR STUDENTS

Diana S. Skowronski*

ABSTRACT

The Children's Online Privacy Protection Act (COPPA) is a federal privacy law that strictly governs how websites collect and distribute personal information from children under the age of thirteen. Children who use Internet sites require additional privacy protections because children may not fully understand the risks associated with releasing their personal information online. Despite recognizing the need for stringent privacy protections for children, a major flaw in the statute's application to schools undercuts the purpose of providing children with an extra layer of protection. The problem is that COPPA does not apply to schools as entities, meaning administrators or teachers can consent to the release of a child's personal information without the child's parent ever knowing. Ultimately, COPPA protections weaken once children step into school and begin using educational websites or technologies at the instruction of their teachers.

COPPA needs reworking, and the statute's shortcomings have become especially clear after the COVID-19 pandemic forced millions of students online. COPPA's school exception makes it a flawed statute to begin with, and its application in an environment where virtual learning and distance education *are the new normal makes COPPA outdated and ineffective. This Note argues for a comprehensive federal*

* Articles Editor, *Georgia State University Law Review*; J.D. Candidate, 2023, Georgia State University College of Law. Special thanks to my faculty advisor Professor Jeffrey Vagle for providing guidance and feedback throughout the entire writing process. Thank you to my family and friends for their continued support and the incredible team from the *Georgia State University Law Review* for their dedicated time and effort preparing this Note for publication.

privacy law with stronger enforcement measures that can withstand changes in technology and its ever-evolving role in our lives.

CONTENTS

INTRODUCTION

There is no comprehensive federal law that regulates Internet privacy protections in the United States.[1] Instead, various federal and state laws address online privacy issues in a disconnected way, leaving certain data collection practices overlooked and unregulated.[2] Generally, Internet privacy laws are a division of the "larger world of data privacy" that seeks to protect Internet users from exposure of sensitive information (including exposure of their personal information and other confidential data, such as financial information).[3] Privacy laws exist because "[e]very time you visit a website, enter your credit or debit card information, sign up for an account, give out your email, fill out online forms, post on social media, or store images or documents in cloud storage, you are releasing personal information into cyberspace."[4] Your digital footprint is everywhere.[5]

But what about children and their personal information? Surely young children are not engaging in sophisticated Internet activities

1. *Internet Privacy Laws Revealed — How Your Personal Information Is Protected Online*, THOMSON REUTERS [hereinafter *Internet Privacy Laws Revealed*], https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online [https://perma.cc/APL3-ECE4] ("There is no single law regulating online privacy."); Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/3C9R-9897] ("[T]here's no single, comprehensive federal law regulating how most companies collect, store, or share customer data.").

2. *See Internet Privacy Laws Revealed*, *supra* note 1. The article describes Internet privacy protection laws in the United States as a "patchwork" of federal and state statutes, further emphasizing that there is no unified approach to regulating how website operators collect personal information from users online. *Id.* Federal laws currently regulate areas concerning unfair and deceptive commercial practices, electronic communications, unlawful computer-related activities, unsolicited commercial emails, and data collection by financial institutions. *Id.* States have also adopted privacy laws including consumer protection statutes, laws protecting categories of personal information, information securities laws, and data breach laws. *Id.*

3. *See Internet Privacy Laws Revealed*, *supra* note 1; *see also What is Data Privacy?* STORAGE NETWORKING INDUS. ASS'N, https://www.snia.org/education/what-is-data-privacy [https://perma.cc/4YP3-VRJP].

4. *Internet Privacy Laws Revealed*, *supra* note 1; Thorin Klosowski, *How to Protect Your Digital Privacy*, N.Y. TIMES, https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy [https://perma.cc/74NX-XG3S] ("Companies and websites track everything you do online. Every ad, social network button, and website collects information about your location, browsing habits, and more. The data collected reveals more about you than you might expect.").

5. *Internet Privacy Laws Revealed*, *supra* note 1.

such as online banking; so, are children personally at risk when they use the Internet for games or education purposes?[6] This Note argues that the answer is yes. After Congress started recognizing privacy risks during the late 1990s that directly affected children, it enacted the Children's Online Privacy Protection Act (COPPA), which gives special online privacy protections to children.[7] Although children use the Internet for less sophisticated purposes, online privacy restrictions for children under COPPA are "stricter than those governing data about older people" because children (being young and impressionable) are "particularly vulnerable" to cybersecurity attacks.[8]

Despite being a stricter privacy rule in theory, COPPA is criticized for being weakly enforced and generally ineffective.[9] One concerning gap in privacy protections is that COPPA does not apply to schools as entities; if a school contracts with an educational website or technology for its students, the school can consent for that website or

6. *See Internet Privacy: Prepared Statement of the Fed. Trade Comm'n Before the Subcomm. on Cts. & Intell. Prop. of the H. Comm. on the Judiciary* (Mar. 26, 1998) [hereinafter *Medine FTC Prepared Statement*] (statement of David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission) ("These young people are not shopping or banking online, but parents still have serious concerns about the online collection and use of personal information from children."); *see also Internet Use in Children*, AM. ACAD. OF CHILD & ADOLESCENT PSYCHIATRY, https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-Online-059.aspx [https://perma.cc/C3DT-HJCR] (Oct. 2015). Young children do not use the Internet for the same purposes as adults. *Id.* Instead, "[m]ost online services give children resources such as encyclopedias, current events coverage, and access to libraries and other valuable material." *Id.* "They can also play games and communicate with friends on social media platforms like Facebook, Twitter, Snapchat, etc." *Id*.

7. *Medine FTC Prepared Statement*, *supra* note 6; 15 U.S.C. § 6501.

8. Josh Fruhlinger, *COPPA Explained: How This Law Protects Children's Privacy*, CSO (Feb. 8, 2021, 2:00 AM), https://www.csoonline.com/article/3605113/coppa-explained-how-this-law-protects-childrens-privacy.html [https://perma.cc/NDV3-QEVP]; *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020) [hereinafter *Complying with COPPA*], https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 [https://perma.cc/M3M9-NDWP].

9. *See What's Going on with the Children's Online Privacy Protection Act (COPPA)?*, OSANO (Jan. 14, 2021), https://www.osano.com/articles/whats-new-coppa [https://perma.cc/G3XE-LPXY]. COPPA enforcement "should be tougher on giant technology companies that violate the law." *Id.* Anna O'Donnell, *Why the VPPA and COPPA Are Outdated: How Netflix, YouTube, and Disney+ Can Monitor Your Family at No Real Cost*, 55 GA. L. REV. 467, 470 (2020). COPPA's "enforcement procedures are lacking." *Id.* Lauren A. Matecki, *Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era*, 5 NW. J.L. & SOC. POL'Y 369, 370 (2010) ("[C]ommentators have criticized COPPA as ineffective.").

technology to collect students' information.[10] In practice, schools release students' personal information without parental consent simply because COPPA does not apply to schools.[11]

In the wake of the COVID-19 pandemic, which has seen a massive shift to online learning, COPPA's inapplicability to schools is a cause for concern.[12] Because the pandemic resulted in nationwide school closures, school districts "rac[ed]" to provide students with distance learning and virtual education options as a substitute for in-person learning.[13] As a result, the unprecedented increase in educational technologies is bringing "more issues and threats in terms of cybersecurity."[14] Now, we are left with millions of students using online education technology services in a world of heightened cybersecurity threats, yet the existing privacy statute enacted two decades ago does little to address this predicament.[15]

---

10. *See Complying with COPPA*, *supra* note 8. The Federal Trade Commission's (FTC) "Frequently Asked Questions" page explains that, under COPPA, schools can allow website operators to collect personal information from students:

> Many school districts contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system – for example, homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. In these cases, the schools may act as the parent's agent and can consent under COPPA to the collection of kids' information on the parent's behalf.

Id.; K-12 BLUEPRINT, EVERYTHING YOU ALWAYS WANTED TO KNOW ABOUT COPPA 1 (2014), https://www.k12blueprint.com/sites/default/files/COPPA-101.pdf [https://perma.cc/LBN8-ZAL8] ("COPPA does not, however, apply to 'school districts that contract with websites to offer online programs solely for the benefit of their students.'").

11. *See* Benjamin Herold, *COPPA and Schools: The (Other) Federal Student Privacy Law, Explained*, EDUC. WK. (July 28, 2017), https://www.edweek.org/technology/coppa-and-schools-the-other-federal-student-privacy-law-explained/2017/07 [https://perma.cc/GR4E-L6JC].

12. Anisha Reddy & Amelia Vance, *Social (Media) Distancing: Online Learning During a Pandemic*, STUDENT PRIV. COMPASS (Mar. 31, 2020), https://studentprivacycompass.org/social-media-distancing-covid19/ [https://perma.cc/3VG9-Q6QL].

13. *Id.*

14. NAVID ALI KHAN, SARFRAZ NAWAZ BROHI & NOOR ZAMAN, TEN DEADLY CYBER SECURITY THREATS AMID COVID-19 PANDEMIC (2020) ("With the advancement of technology, nowadays, cybersecurity has become very challenging. It's common for hackers, attackers, and scammers to take advantage of emergencies, particularly in times when people are frightened, desperate, and most vulnerable. The outbreak of coronavirus is no different. Bad actors around the world are using the coronavirus as a new tool for their evil deeds in the form of hacking, attacking, or scams.").

15. *See* Lisa Weintraub Schifferle, *COPPA Guidance for Ed Tech Companies and Schools During the Coronavirus*, FED. TRADE COMM'N (Apr. 9, 2020, 8:18 AM), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus [https://perma.cc/H8KH-XYGD].

Part I of this Note explains COPPA's origins and how the statute requires the Federal Trade Commission (FTC) to enforce COPPA's regulations for protecting children's online privacy. Part II analyzes COPPA's shortcomings in the realm of educational technologies. In Part III, the Author proposes a COPPA overhaul in favor of a comprehensive federal privacy law to protect children's personal information in virtual education settings.

I. BACKGROUND

By the 1990s, 9.8 million children were going online for activities like "homework or informal learning, playing games, browsing or for e-mail/chat rooms," and parents developed concerns about their children's personal information being collected and used.[16] Congress therefore enacted COPPA to restrict website operators from soliciting personal information from children and to give parents control over the information that website operators collected from their children online.[17] The COPPA statute limits online privacy protection to children who are under thirteen years old, reasoning that "children under the age of thirteen do not have the developmental capacity to understand the nature of a website's request for information and its privacy implications."[18] The idea is that children lack the ability to meaningfully consent to the release of their personal information

16. *Medine FTC Prepared Statement*, *supra* note 6 (statement of David Medine) ("Several workshop participants voiced concern at the 1997 Workshop about online activities that enable children to post or disclose their names, street addresses, or e-mail addresses in areas accessible to the public, such as chat rooms, bulletin boards, and electronic pen pal programs, creating a serious risk that the information may fall into the wrong hands.").

17. *Complying with COPPA*, *supra* note 8. The FTC's "Frequently Asked Questions" page explains that Congress enacted COPPA in 1998, which went into effect in 2000, and that the main goal of COPPA is to put parents in control of how website operators collect information from young children online. *Id.*; *History of COPPA Violations*, PRIVO, https://www.privo.com/history-of-coppa-violations [https://perma.cc/58UU-JMKY] ("COPPA was enacted by the United States in 1998, and became effective on April 21, 2000. The FTC enforces violations concerning children's online privacy and state attorneys general."); 2 TELECOMMUNICATIONS REGULATION: CABLE, BROADCASTING, SATELLITE, AND THE INTERNET ¶ 17C.03 (Matthew Bender & Co. 2022).

18. 15 U.S.C. § 6501; Joshua Warmund, Note, *Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 189, 190 (2000).

without parental involvement.[19] One website in particular, KidsCom, gained negative attention during the 1990s for collecting information from children who did not fully understand what was happening to their personal information, and it was KidsCom's practices that led to COPPA's enactment.[20]

A. COPPA's Origins

KidsCom, "one of the [I]nternet's first child-focused sites," caught the attention of the Center for Media Education in the 1990s.[21] At the time, KidsCom collected children's personal information through registration forms, contests, and pen-pal programs.[22] The Center for Media Education drafted a petition urging the FTC to investigate KidsCom's information collecting practices, which the organization claimed were in violation of Section 5 of the Federal Trade Commission Act (FTC Act).[23] The FTC is the relevant federal agency to investigate such concerns because it is tasked with protecting consumers by stopping unfair, deceptive, or fraudulent practices that occur in the marketplace, and it has authority to conduct investigations, sue companies that violate the law, and create rules to protect the marketplace.[24] Section 5(a) of the FTC Act, which the Center for

---

19. *See* Alexis M. Peddy, *Dangerous Classroom "App"-titude: Protecting Student Privacy from Third-Party Educational Service Providers*, 2017 BYU EDUC. & L.J. 125, 132 (2017).

20. *See* Fruhlinger, *supra* note 8.

21. *Id.*

22. *Id.*; *see also How COPPA Came About*, INFORMATIONWEEK (Jan. 14, 2004), https://www.informationweek.com/it-life/how-coppa-came-about [https://perma.cc/Z9HK-4G2K]. The article provides an overview of how KidsCom collected data from young children:

> Online since February 1995, KidsCom was one of the first children-only sites on the Internet. It didn't use cookies to gather information, but collected data through registration forms, contests, and pen-pal programs. Its site was directed at children from ages four to [fifteen] and came under criticism for its collection practices.

Id.

23. *Protection of Children's Privacy on the World Wide Web: Prepared Statement of the Fed. Trade Comm'n Before the Subcomm. on Commc'ns of the S. Comm. on Com., Sci. & Transp.* (Sept. 23, 1998) [hereinafter *Pitofsky FTC Prepared Statement*] (statement of Robert Pitofsky, Chairman, Federal Trade Commission).

24. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do [https://perma.cc/X38L-5VUU]; *A Message from Chairwoman Edith Ramirez*, FED. TRADE COMM'N (2012), https://www.ftc.gov/reports/ftc-2013/message-chairwoman-edith-ramirez [https://perma.cc/JDB9-N47Y] ("The FTC is a bipartisan federal agency with a unique dual mission to

Media Education claimed KidsCom was violating, gives the FTC the power to initiate enforcement actions when "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful."[25]

The FTC investigated KidsCom's data collection practices and responded in a staff opinion letter (KidsCom Letter), where it shared its determination that KidsCom violated FTC rules.[26] The FTC urged website operators to include parental notices on their websites and to require parental consent before releasing personally identifying information to third parties.[27] By making these recommendations via the KidsCom Letter, "the FTC publicly announced its guidelines for data collection from children on the Internet for the first time."[28] Less than a year following the KidsCom Letter, the FTC presented a report before Congress detailing its concerns surrounding the online collection of children's personal information and the need for parental involvement in personal information disclosures.[29] Following the FTC's report, as well as an FTC public workshop consisting of industry representatives (including website operators and technology companies) debating privacy law issues, Congress officially enacted COPPA in 1998.[30]

---

protect consumers and promote competition . . . the FTC is dedicated to advancing consumer interests while encouraging innovation and competition in our dynamic economy."); *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N [hereinafter *Overview of FTC Authority*], https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/38KN-HP7Y] (May 2021).

25. *Overview of FTC Authority*, *supra* note 24. FTC has investigative, enforcement, and rulemaking authority to protect consumers and promote competition, and its authority is derived from the Federal Trade Commission Act. *Id.*

26. Fruhlinger, *supra* note 8; Press Release, Fed. Trade Comm'n, FTC Staff Sets Forth Principles for Online Information Collection from Children (July 16, 1997), https://www.ftc.gov/news-events/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection [https://perma.cc/Z5DA-SP77]; *Pitofsky FTC Prepared Statement*, *supra* note 23 (statement of Robert Pitofsky). Pitofsky's statement identifies a deceptive practice to misrepresent the reason for collecting personal data from children, such as claiming that information is being collected for a contest despite it being collected for a mailing list, which constitutes a violation of FTC rules. *Id.*

27. Rajiv Ch & rasekaran, *FTC Rules on Online Data Collection*, WASH. POST (July 17, 1997), https://www.washingtonpost.com/archive/business/1997/07/17/ftc-rules-on-online-data-collection/a7e3ab7f-8deb-4613-8ae0-a48eda19f466/ [https://perma.cc/T4KX-5VDY].

28. Warmund, *supra* note 18, at 193.

29. *See Medine FTC Prepared Statement*, *supra* note 6.

30. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888-01, 59,888 (Nov. 3, 1999) (to be codified at 16 C.F.R. pt. 312). In addition to industry representatives, around 100 other

B. COPPA Requirements and its Enforcement Process

COPPA prohibits commercial website operators and online services operators from collecting children's personal information from websites that are either directed at children under thirteen years old or from websites where operators have actual knowledge that children use their sites.[31] To comply with COPPA, website operators must take specific measures to clearly communicate how they collect personal information, and they must obtain parental consent before collecting and using this data.[32]

The type of "personal information" protected under COPPA includes names, addresses, online contact information, screen names or usernames, telephone numbers, Social Security numbers, files containing the child's picture or voice, geolocation information, or information that an operator can combine with an identifier to recognize the user.[33] If website operators collect this personal information without parental consent, the FTC has the authority to

parties—including privacy advocates, consumer groups, and other government agency representatives—attended the FTC public workshop. *Id.* The purpose of the workshop was to discuss how parental consent was currently being obtained, how email could be implemented to obtain consent, and whether other methods of obtaining parental consent could be used in the future. *Id.*; 15 U.S.C. § 6501.

31. § 6501; *Complying with COPPA*, *supra* note 8. COPPA requirements apply not only to child-focused websites but also to websites with general audiences where website operators have actual knowledge that they are collecting personal information from children ages thirteen and under. *Id.*

32. *See Complying with COPPA*, *supra* note 8. Specifically, to comply with COPPA, website operators must first post an online privacy policy describing their information collection practices. *Id.* Second, operators must provide notice directly to parents and obtain their consent before collecting personal information from their children. *Id.* Third, website operators must give parents the option of consenting to the data collection while "prohibiting the operator from disclosing that [data] to third parties." *Id.* Next, website operators must give parents access to their children's personal information to review or delete the data. *Id.* Operators must also allow parents to prevent any further use or collection of their children's information. *Id.* Website operators must maintain the "confidentiality, security, and integrity of information they collect from children" and can only retain the information for as long as it is needed to fulfill the purpose for collecting it. *Id.* Finally, website operators cannot "condition a child's participation in an online activity on the child providing more information than is reasonably necessary to participate in that activity." *Id.*

33. INTERACTIVE ADVERT. BUREAU, GUIDE TO NAVIGATING COPPA 4 (2019); *Complying with COPPA*, *supra* note 8; Chrissie Scelsi, *Children's Online Privacy Protection*, 37 GPSOLO, Sept./Oct. 2020, at 42, 43–44; Sean Meyers, *Guide to COPPA*, PRIV. POL'YS, https://www.privacypolicies.com/blog/coppa/ [https://perma.cc/Z4FW-NJZL] (May 20, 2021) ("What constitutes 'personal information' is far-reaching and not just limited to things like Social Security numbers and bank account information.").

enforce COPPA and hold website operators liable for civil penalties.[34] Regarding enforcement practices, if the Attorney General fails to initiate litigation for COPPA violations after notice from the FTC, "[t]he FTC is . . . authorized to initiate federal district court proceedings, by its own attorneys, to recover civil penalties for violations of the COPPA Rule."[35]

Despite the FTC having full enforcement authority, commentators have criticized it for weakly enforcing COPPA.[36] Ultimately, "its enforcement has resulted in small settlements with companies that have been charged with collecting children's private information."[37] For example, it took roughly twenty years since COPPA's enactment to see a historic settlement between YouTube and the FTC for $170 million in 2019.[38]

---

34. *Complying with COPPA*, *supra* note 8; *The Children's Online Privacy Protection Act (COPPA)*, PRIVO, https://www.privo.com/learn-more-about-coppa [https://perma.cc/U3J4-KS3M] ("COPPA provides the FTC with civil penalty authority to encourage compliance with the COPPA Rule. The FTC has taken law enforcement action against companies that failed to comply with the provisions of the law. A court can hold operators who violate the Rule liable for civil penalties of up to $41,484 per violation.").

35. Complaint at 4, Fed. Trade Comm'n v. Google, LLC (No. 19-cv-2642) (D.D.C. Sept. 4, 2019); Benjamin Stein, *Plaintiffs Continue Search for De Facto COPPA Right of Action*, INFOLAWGROUP (Mar. 25, 2020), https://www.infolawgroup.com/insights/2020/3/23/plaintiffs-continue-search-for-de-facto-coppa-right-of-action [https://perma.cc/4YLD-7FZ9]. Because COPPA enforcement authority is vested solely in the FTC and state Attorneys General, there is no private right of action for COPPA violations. *Id.* As a result, parents cannot bring COPPA actions if their children's personal information is collected and used without consent. *See id.* Parents must therefore rely entirely on the FTC to ensure that website operators are complying with COPPA's requirements. *See id.*

36. O'Donnell, *supra* note 9. O'Donnell describes the FTC's poor COPPA enforcement history:

> As of 2020, over two decades since COPPA was originally enacted, no company charged by the FTC has ever been taken to court for violating COPPA. This is not because COPPA sees no action—on the contrary, COPPA is enforced, albeit weakly, quite often. Instead, the dearth of trials exists because the FTC has settled every one of its thirty complaints against companies for violating COPPA.

Id. at 481. (citations omitted).

37. *Id.* at 467.

38. *See* Lesley Fair, *$170 Million FTC-NY YouTube Settlement Offers COPPA Compliance Tips for Platforms and Providers*, FED. TRADE COMM'N BUS. BLOG (Sept. 4, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/09/170-million-ftc-ny-youtube-settlement-offers-coppa [https://perma.cc/FN6G-PFMV]; *see also* O'Donnell, *supra* note 9, at 488; Complaint, *supra* note 35, at 6, 8–10. The Complaint alleged that Google and YouTube violated COPPA in several ways: by not requiring users to create accounts, by marketing popular brands of children's products and services, by classifying certain videos and channels as "Made for Kids," by creating a mobile app called "YouTube Kids," by hosting child-directed channels, and by engaging in other kid-focused practices without disclosing their data collection practices and first obtaining parental consent. *Id.* at 9, 16–17; Natasha Singer & Kate Conger, *Google Is Fined $170 Million for Violating Children's Privacy on YouTube*, N.Y.

C. The 2013 Amended COPPA Rule

The gradual increase in COPPA settlement amounts may be attributed to COPPA's 2013 amendment.[39] To address changes in children's use and access to the Internet through technologies like cell phones and social media sites, the FTC revised COPPA to expand the definition of "personal information" and to give parents additional control over the collection of their children's data.[40] The FTC created these changes pursuant to the agency's rulemaking authority; under the FTC Act, the FTC has exclusive authority to issue rules related to unfair or deceptive acts or practices.[41]

Despite the 2013 update, "technological advances and a shift in marketing practices have called into question the practicality of, and compliance with, COPPA's parental consent and personal information collection requirements."[42] Even though fines for violating COPPA are becoming greater over time, there are lingering concerns

---

TIMES, https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html [https://perma.cc/MRM4-KTER] (Aug. 10, 2021). The news article further explains the allegations against Google and YouTube and how YouTube profited from its conduct:

> Regulators said that YouTube, which is owned by Google, had illegally gathered children's data—including identification codes used to track web browsing over time—without their parents' consent. The site also marketed itself to advertisers as a top destination for young children, even as it told some advertising firms that they did not have to comply with the children's privacy law because YouTube did not have viewers under [thirteen]. YouTube then made millions of dollars by using the information harvested from children to target them with ads . . . .

Id.

39. *See* Press Release, Fed. Trade Comm'n, Revised Children's Online Privacy Protection Rule Goes into Effect Today (July 1, 2013), https://www.ftc.gov/news-events/press-releases/2013/07/revised-childrens-online-privacy-protection-rule-goes-effect [https://perma.cc/A2W8-DZK6].

40. *Id.*

41. *Overview of FTC Authority*, *supra* note 24. The FTC has rulemaking authority under the FTC Act:

> In lieu of relying on actions against individual respondents to determine that practices are unfair or deceptive, the Commission may use trade regulation rules to address unfair or deceptive practices that occur commonly.
>
> . . . .
>
> Under Section 18 of the FTC Act, 15 U.S.C. Sec. 57a, the Commission is authorized to prescribe "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce" within the meaning of Section 5(a)(1) of the Act.

Id.

42. Kathryn Beaumont Murphy, Meghan Talbot, Jillian Walton, Saul Ewing Arnstein & Lehr LLP, *FTC Explores Changes to COPPA Rule*, JDSUPRA (Oct. 11, 2019), https://www.jdsupra.com/legalnews/ftc-explores-changes-to-coppa-rule-16445/ [https://perma.cc/CR57-9M5Q].

surrounding COPPA's applicability and enforcement as technology continues to change rapidly, especially in the wake of the COVID-19 pandemic.[43]

D. COPPA in the Realm of Educational Technologies

In 2019, even before the COVID-19 pandemic began, the FTC again recognized the need to update COPPA.[44] Although the FTC did not intend to fully update COPPA in 2019, it began requesting public comments about the statute as part of the FTC's rulemaking authority.[45] By doing so, the FTC began its COPPA review process years earlier than expected, in part because of changes occurring in educational technologies.[46] The collection of children's personal data in the education space is especially problematic because COPPA and its protections do not apply directly to schools.[47] When schools contract with website operators, the institutions are able to consent to

43. *See History of COPPA Violations*, *supra* note 17. Per the timeline of significant COPPA violations and their settlement amounts, the FTC filed its first complaint for a COPPA violation against Toysmart.com in 2000, after the company collected personal information and attempted to sell this information with its assets when it ran into financial difficulty. *Id.* The most recent complaint over a COPPA violation, according to the timeline, was against Recolor in 2021 for allowing third-party advertising networks to collect personal information from the app's social media features for targeted ads, which settled for $3 million. *Id.*; O'Donnell, *supra* note 9 ("The Federal Trade Commission (FTC) has updated COPPA for modern technology and privacy concerns, but its enforcement procedures are lacking.").

44. *See* Lesley Fair, *Future of the COPPA Rule: What's on the Agenda*, FED. TRADE COMM'N BUS. BLOG (Oct. 1, 2019, 11:46 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/10/future-coppa-rule-whats-agenda [https://perma.cc/BRY3-V8YE] ("Whether it's social media, the Internet of Things, or educational technology, do changes in media and the marketplace warrant updates to the Rule? The FTC staff asked that question . . . .").

45. Murphy et al., *supra* note 42 ("The FTC is not yet considering specific changes to COPPA, but as part of its rulemaking process it is soliciting opinion and commentary about the current state of the law—its successes and challenges—which may result in further amendments to the law."); Lesley Fair, *COPPA Comment Deadline Extended to December 11th*, FED. TRADE COMM'N BUS. BLOG (Dec. 10, 2019, 9:56 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/12/coppa-comment-deadline-extended-december-11th [https://perma.cc/AW98-UQV5].

46. *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 Fed. Reg. 35,842, 35,842 (July 25, 2019) (to be codified at 16 C.F.R. pt. 312). The FTC usually does a ten-year review of its rules to keep up with marketplace and technology changes. *Id.* The previous COPPA review ended in 2013, but the FTC began its review of COPPA early in 2019, citing questions about the Rule's application "to the educational technology sector, to voice-enabled connected devices, and to general audience platforms that host third-party child-directed content." *Id.*

47. Peddy, *supra* note 19, at 130 ("COPPA does not apply directly to schools as entities."); Herold, *supra* note 11 ("This law directly regulates companies, not schools.").

a website's collection of personal information from students, which removes parents' ability to consent to this data collection.[48] The COVID-19 pandemic has only complicated matters further.[49]

Because the pandemic resulted in nationwide school closures, students had to switch to virtual learning and distance education options.[50] The unprecedented, steep increase in young children using educational technologies has created significant privacy concerns.[51] In recognition of the effect that increased education technology usage would have on COPPA compliance, the FTC created a blog post in April 2020 with guidance on how education technology companies and schools can stay COPPA compliant during the transition to remote learning.[52] Within the blog post, the FTC acknowledged that "millions of students are now using online, educational technology (or 'ed tech') services to engage in remote learning" and stressed the importance of the "continued need to protect student's privacy."[53] This acknowledgment reveals that the FTC is at least aware of the privacy

48. *Complying with COPPA*, *supra* note 8.

49. *See* Peggy Keene, *Virtual Classes: The Rush for Online Schooling Has Raised Privacy Concerns*, 83 TEX. BAR J. 370, 370 (2020).

50. *See* Reddy & Vance, *supra* note 12; *see also* Cathy Li & Farah Lalani, *The COVID-19 Pandemic Has Changed Education Forever. This is How*, WORLD ECON. F. (Apr. 29, 2020), https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/ [https://perma.cc/3BH8-DCXJ]. Before COVID-19, the adoption of education technology was already growing, but there has been "a significant surge in usage since COVID-19." *Id.* The COVID-19 pandemic has resulted in a "distinctive rise of e-learning." *Id.*; KHAN ET AL., *supra* note 14 ("To limit the spread of this novel disease, many countries decided to close educational institutions, including schools, colleges, and universities. Lecturers are teaching online; in fact, this is happening at a very huge untested and unprecedented scale.").

51. *See* Tiffany C. Li, *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, 52 LOY. U. CHI. L.J. 767, 775 (2021) ("Most of the technologies being deployed as COVID-19 responses are not new. . . . [T]he novelty of new technologies is not what matters for understanding how the law should regulate. Rather, it is what has changed in society that has driven the rise in certain technologies that we should seek to understand."). Li stresses that the technologies people are using have not changed. *Id.* Instead, the important factor that is causing additional problems is the steep increase in their usage. *Id.*; KHAN ET AL., *supra* note 14. Khan states that "[t]he online video conferencing apps such as Zoom, Microsoft Teams, and Google Meet have witnessed an exponential increase in new users signing up daily," even though Zoom, Microsoft Teams, and Google Meet are not brand-new technologies born out of the COVID-19 pandemic. *See id.*

52. Schifferle, *supra* note 15. The FTC repeatedly stresses in its blog post that "COPPA does not impose obligations on schools" and simply advises education-technology companies and schools on how to maintain their COPPA compliance. *Id.* The blog post gives off the impression that the FTC's primary focus is providing guidance for companies to avoid liability under COPPA rather than making children's privacy rights the FTC's primary objective. *See id.*

53. *Id.*

concerns that directly affect students as a group and that the COVID-19 pandemic is exacerbating these already-existing student privacy concerns.[54]

II. ANALYSIS

The FTC acknowledges that protecting student privacy is a pressing issue during the COVID-19 pandemic, yet COPPA requirements do not apply to schools as entities and COPPA protections remain limited to children under the age of thirteen, thus ignoring teenage students.[55] COPPA already had major gaps in privacy protections for students using educational technologies during pre-pandemic times; even before the pandemic began, "advances in technology and telecommunications . . . dramatically changed the landscape of education in the United States." [56] The COVID-19 pandemic is therefore one illustration of COPPA's inadequacies as applied to students and educational technologies in modern times.

A. Online Privacy Protections Are Becoming Increasingly Necessary for Students

Privacy threats and data breaches of K-12 educational institutions are not new.[57] Because students use online services for educational purposes "to access class readings, to view their learning progression, to watch video demonstrations, to comment on class activities, or to complete their homework," these activities put students at risk for

54. *See id.*; R. Chantz Richens, *Privacy in a Pandemic: An Examination of the United States' Response to COVID-19 Analyzing Privacy Rights Afforded to Children Under International Law*, 28 WILLAMETTE J. INT'L L. & DISP. RESOL. 244, 259 (2021) ("Issues of privacy and children, which have been growing in recent years, have all but come to a head as a result of the COVID-19 pandemic.").

55. *See* Schifferle, *supra* note 15; *see also Complying with COPPA*, *supra* note 8; 15 U.S.C. § 6501.

56. PRIV. TECH. ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES 1 (2014), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf [https://perma.cc/6FVG-NU4R].

57. TyLisa C. Johnson, *'The Cameras Are Always On': Student Surveillance and Privacy Protection in the Age of E-Learning*, PUBLICSOURCE (Nov. 19, 2020), https://www.publicsource.org/the-cameras-are-always-on-student-surveillance-and-privacy-protection-in-the-age-of-e-learning/ [https://perma.cc/VW3N-8MQ2].

cyber threats and cyberattacks.[58] Privacy experts explain that "[s]ome threats are old–phishing and ransomware attacks and data breaches–and some are new, birthed strictly from the shift to a virtual learning environment amid COVID-19, such as 'Zoom-bombing,' where an unauthorized person enters and disrupts a Zoom meeting."[59] Ultimately, cybersecurity issues are further disrupting student learning during the COVID-19 pandemic.[60]

Additionally, the collection of personal data from students for the purpose of targeted advertising is a primary concern resulting from students using educational technologies.[61] Website operators collect

---

58. PRIV. TECH. ASSISTANCE CTR., *supra* note 56, at 1–2.

59. Johnson, *supra* note 57; KHAN ET AL., *supra* note 14. Khan addresses widespread concern with the Zoom application:

> [W]ith the rapid growth of Zoom's popularity, Zoom is now faced with massive backlash as security professionals, privacy advocates, lawmakers, and even the FBI warn that Zoom's default settings are not safe. As a result, many companies such as NASA, SpaceX, and countries, including Taiwan, USA, and the Australian Defense force, banned Zoom for communication.

Id.; MARIA CLARE LUSARDI, ISAAC DUBOVOY & JEREMY STRAUB, DETERMINING THE IMPACT OF CYBERSECURITY FAILURES DURING AND ATTRIBUTABLE TO PANDEMICS AND OTHER EMERGENCY SITUATIONS (2020) ("Schools that have turned to remote instruction have faced problems with video conferences being hijacked. The FBI reported that it[] 'has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.'"); Luke Barr, *FBI Warns of Cyberattacks to Distance Learning*, ABC NEWS (Jan. 4, 2021, 4:02 PM), https://abcnews.go.com/Politics/fbi-warns-cyberattacks-distance-learning/story?id=75038470 [https://perma.cc/K2S7-TG6A] ("Another common incident that happens, . . . is 'zoombombing'—a practice where criminals enter an online classroom and post or yell a racist or inflammatory slur."); Michael Goodyear, *The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and the Fragmented State of U.S. Data Privacy Law*, 10 HOUS. L. REV. 76, 77 (2020) ("Zoom's risky and intentionally aggressive privacy practices have led some to conclude that the increased use of Zoom is a 'privacy disaster waiting to happen.'").

60. *See* Alyson Klein, *Cyberattacks Disrupt Learning Even More During COVID-19*, EDUC. WK. (Sept. 14, 2020), https://www.edweek.org/technology/cyberattacks-disrupt-learning-even-more-during-covid-19/2020/09 [https://perma.cc/YX3E-N6Q6]; *see also* Barr, *supra* note 59. Quoting FBI Cyber Section Chief Dave Ring, Barr explains the projected increase in cybersecurity attacks following the move to virtual education:

> The broader the move to distance learning, I think the more attacks you're going to see, just simply because there are more opportunities for it and it's more disruptive . . . . Not everybody's looking to make money when it comes to criminal motivations for these attacks. A lot are [there] looking to steal information.

Id. (statement of Dave Ring, FBI Cyber Section Chief); Alan Butler & Enid Zhou, *Disease and Data in Society: How the Pandemic Expanded Data Collection and Surveillance Systems*, 70 AM. U. L. REV. 1577, 1613 (2021) ("[T]here has . . . been an exponential growth in the collection, use, and dissemination of personal data online as people have become increasingly reliant on remote access to work, school, social services, and other necessities.").

61. *See Complying with COPPA*, *supra* note 8.

personal information from children because "[c]hildren are an attractive audience for marketers because their interest in a product can influence a family's purchasing habits and shape future behaviors."[62] For example, the mobile application "Take With Me Learning," which offers interactive teaching lessons to students, was created by a company that was illegally collecting student data and selling it to advertisers, which made student information fully accessible without limitation.[63] This type of data collection makes students susceptible to criminal activity and exposes students to dangers such as tracking, fraud, harassment, and identity theft.[64] Any failure on COPPA's part to adequately protect students (and not just children under thirteen) from illegal data collection and cybersecurity attacks creates real and irreversible consequences.[65]

Although the COVID-19 pandemic introduced additional privacy threats as a result of increased virtual education measures, student online privacy concerns do not end here; even as the pandemic subsides, educators will continue incorporating aspects of virtual learning in their teaching.[66] At this point, "[i]t is possible that more

62. Olivia Levinson, Note, *Embedded Deception: How the FTC's Recent Interpretation of the Children's Online Privacy Protection Act Missed the Mark*, 105 MINN. L. REV. 2007, 2012 (2021); Matecki, *supra* note 9, at 388 ("Today, one of the most prevalent uses of personal information online is a web operator's ability to create effective and targeted advertising. Online advertising has grown to a nearly ten[-]billion[-]dollar industry in recent years. By using personal information gathered online, marketers can effectively target audiences based on interests, demographics, and any other factor about a person that can be ascertained from web history and online behavior." (citations omitted)); Allison Schiff, *The FTC's Review of COPPA Could Transform How Kids Content Is Monetized Online*, AD EXCHANGER (Oct. 8, 2019, 3:25 PM), https://www.adexchanger.com/privacy/the-ftcs-review-of-coppa-could-transform-how-kids-content-is-monetized-online/ [https://perma.cc/YPY4-76V4] ("It's a misconception that COPPA outlaws targeting children with advertising. It simply imposes certain requirements, particularly the need to get verifiable parental consent for data collection, on the operators of websites or online services directed at children under [thirteen].").

63. Peddy, *supra* note 19, at 126.

64. *Id.* at 128–29.

65. *See id.* at 130.

66. *See* Jessica Dickler, *Post-pandemic, Remote Learning Could Be Here to Stay*, CNBC, https://www.cnbc.com/2020/05/20/post-pandemic-remote-learning-could-be-here-to-stay.html [https://perma.cc/MFS2-7L4H] (May 26, 2020, 12:56 PM); *see also* Tiffany C. Li, *Post-pandemic Privacy Law*, 70 AM. U.L. REV. 1681, 1712 (2021). Because schools will likely continue using distance education technologies even after the COVID-19 pandemic slows down, "[w]hatever laws and legal norms we create to address this pandemic will not be isolated to this pandemic." *Id.*; Li, *supra* note 51, at 859. Similarly, "[s]ociety must protect the health of its people, but we must remain vigilant about privacy incursions[]

schools will rely on distance education in the future, perhaps due to familiarity gained by faculty, staff, and students during the pandemic."[67] Students will transition back to primarily in-person classes; however, schools will still implement educational technologies and thus continue exposing students to illegal data collection and cyber threats.

B. COPPA's Shortcomings in Protecting Students from Privacy Threats

Overall, COPPA's "lack of enforcement has rendered COPPA's application to schools unclear and unworkable."[68] As explained in Part I, COPPA and its protections do not directly apply to schools.[69] Schools can thus give consent on behalf of parents to release their children's information, meaning that schools put themselves in the middle of the relationship between website operators and parents.[70] Regarding the mobile application "Take With Me Learning," parents discovered that their children's schools required students to use this application, but the schools circumvented their parental consent in its dealings with the application operator, subjecting students to the

---

because shifts in privacy norms now will lead to lasting repercussions even after the emergency has ended." *Id.* Legal scholars are stressing the fact that looking to the future in a post-pandemic world is essential when considering how technology is used and how changes in privacy law apply to the new normal. *See id.*

67. Li, *supra* note 51, at 794.

68. Peddy, *supra* note 19, at 131; O'Donnell, *supra* note 9, at 469, 470.

69. *See supra* Part I.

70. Herold, *supra* note 11; Peddy, *supra* note 19, at 136 ("In application, COPPA requires that before a third-party operator authorizes a child under thirteen to use its website and services, it must provide notice and obtain verifiable parental consent. However, operators contracted within the school setting must provide such notice directly to the school, not to the parent."). *But see* Jennifer Thompson, *School or Parent? Factors Playing into the FTC's Analysis of Who Should Provide Parental Consent Under COPPA in the Age of EdTech*, JDSUPRA (Mar. 12, 2020), https://www.jdsupra.com/legalnews/school-or-parent-factors-playing-into-69062/ [https://perma.cc/2MTX-LQGS]. Thompson describes the practical effects of requiring every single parent to approve education technologies for their children:

> From a purely administrative point of view, the schools have a compelling argument for being able to provide consent for the community. If individual families are required to provide the consent, not only would the schools have to track which family has approved which EdTech technology, the schools would also have to come up with alternative curriculum options for students that do not want to use the available EdTech.

Id.

collection and distribution of their personal information for targeted advertising purposes.[71] The "Take With Me Learning" example is not an isolated incident; schools often circumvent parental consent in practice.[72]

Additionally, "many educators have not been apprised of the risks and legal ramifications of using . . . online schooling methods without first securing proper permission from parents or guardians."[73] So, not only does COPPA not apply directly to schools as entities but educators are typically unaware of the privacy consequences associated with implementing educational technologies without getting parental permission.[74] Students, especially teenagers, are therefore left with privacy protections that do not apply to their educational institutions and are ultimately disregarded by their educators.[75] As a result, "a gap exists between the protection of a child's privacy at home and a child's privacy while at school."[76] This gap highlights COPPA's inadequacies when applied in the context of educational technologies and distance-learning tools.

C. COPPA's "Educational Context" Limitation

Although COPPA does not apply to schools as entities, whether a school can grant COPPA consent on behalf of parents "varies under certain circumstances."[77] The FTC explains that "the school's ability

71. Peddy, *supra* note 19, at 126–27.

72. *See* Herold, *supra* note 11.

73. Keene, *supra* note 49.

74. *See id.*; Peddy, *supra* note 19, at 157. Because educators are usually unaware of the dangers that stem from implementing educational technologies without first obtaining parental consent for data collection, legal scholars have suggested requiring teachers or school administrators to complete a certified student-data privacy course annually to help minimize confusion surrounding data privacy in educational technologies. *Id.*; Cameron Sullivan, *How COPPA Affects Schools*, LEARNSAFE (Nov. 18, 2019), https://learnsafe.com/how-coppa-affects-schools/ [https://perma.cc/J3F3-TG6D] ("Teachers need to be aware of what COPPA requires for the technology and sites they use in the classroom. Sometimes, a teacher can provide the necessary consent. This is somewhat of a grey area. It's often hard to know in what circumstances teachers can give consent.").

75. *See* Keene, *supra* note 49.

76. Peddy, *supra* note 19, at 136.

77. *See* Herold, *supra* note 11 (statement of Bill Fitzgerald, Director of Privacy-Evaluation Initiatives, Common Sense Media); Sullivan, *supra* note 74. Schools granting consent on behalf of parents is not a straightforward process:

to consent for the parent is limited to the educational context—where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose."[78] Schools are thus not allowed to grant consent on behalf of parents if website operators are collecting information from children for purposes that are unrelated to education.[79] The FTC's reasoning behind this determination is that "the scope of the school's authority to act on behalf of the parent is limited to the school context."[80] Although this limitation appears to fully protect students from having their personal information used and disclosed while using educational technologies, in practice that is not always the case.[81]

First, COPPA's educational context limitation does little to protect students because website operators embed third-party trackers into their sites for analytics and advertising purposes.[82] Third-party tracking refers to a website allowing other companies to collect

> COPPA requires sites to obtain parental consent before collecting or using data from users under the age of [thirteen]. If students access the [I]nternet for class, schools and teachers may have to take on this responsibility. Schools may have to ask for verifiable parental consent on the site's behalf, give consent in place of a parent, or request the deletion of collected data. However, the law does not always make it clear how the consent has to be obtained. Some schools may simply send home a note asking for parental consent for [I]nternet use in the classroom. This wouldn't be the appropriate level of consent. Teachers need to list specific sites and what information they gather.

Id.; Thompson, *supra* note 70 ("Some educators have called for additional direction from the FTC as to when schools can provide consent, what obligations service providers have and what rights parents have with respect to information collected from students.").

78. *Complying with COPPA*, *supra* note 8. The FTC recommends that schools ask potential operators the following questions before entering into an agreement that allows for student data collection:

> What types of personal information will the operator collect from students? How does the operator use this personal information? Does the operator use or share information for commercial purposes not related to the provision of the online services requested by the school? . . . Does the operator enable the school to review and have deleted the personal information collected from their students? . . . What measures does the operator take to protect the security, confidentiality, and integrity of the personal information it collects? What are the operator's data retention and deletion policies for children's personal information?

Id.

79. *See* Herold, *supra* note 11.

80. *Complying with COPPA*, *supra* note 8.

81. *See* Herold, *supra* note 11.

82. *Id.*

information from Internet users to deliver targeted advertisements.[83] Even though the FTC requires that operators disclose these tracking services to schools, "vendors often don't provide that information to schools, or do so only in vague or conditional terms."[84] Additionally, regarding the COPPA statute, "its language generates confusion about which third-party operators must follow regulations for online privacy and who is at risk for sanctions if they don't comply."[85]

The third-party tracking practice is problematic in educational technologies because, for example, Zoom allows third parties to access student data, and thousands of schools nationwide adopted the Zoom platform for virtual education purposes as a result of the COVID-19 pandemic.[86] Even though a school's ability to consent for the parent is limited to education purposes, the school may still be allowing student data collection without consent if site operators do not disclose third-party tracking.

Another reason the educational context limitation is ineffective is because the websites and services that schools require students to use often have overlapping educational and commercial applications.[87]

---

83. *How to Protect Your Privacy Online*, FED. TRADE COMM'N (May 2021), https://www.consumer.ftc.gov/articles/how-protect-your-privacy-online [https://perma.cc/79TC-NA56]; *All You Need to Know About Third-Party Cookies*, COOKIE SCRIPT BLOG, https://cookie-script.com/all-you-need-to-know-about-third-party-cookies.html [https://perma.cc/SC2U-WB5B] (Dec. 21, 2021). The following is an example of how third-party trackers collect information to deliver targeted advertisements:

> Let's say earlier in the week you looked up some vacation rentals in Cancun. You browsed a few websites, admired the photos of the sunsets and sandy beaches, but ultimately decided to wait another year before planning your vacation. A few days go by and suddenly it seems like you are seeing ads for Cancun vacations on many websites you visit. Is it a mere coincidence? Not really. The reason you are now seeing these ads on vacationing in Cancun is that your web browser stored a third-party cookie and is using this information to send you targeted advertisements.

Id.

84. *See* Herold, *supra* note 11.

85. Peddy, *supra* note 19, at 130; *All You Need to Know About Third-Party Cookies*, *supra* note 83. In addition to Zoom using third-party trackers, if students use any website that shows advertisements, they can reasonably expect that website to have first- and third-party cookies collecting information. *See All You Need to Know About Third-Party Cookies*, *supra* note 83.

86. Cheri Kiesecker, *What You Need to Know About Zoom for Education*, STUDENT PRIV. MATTERS: PARENT COAL. FOR STUDENT PRIV. BLOG (Aug. 11, 2020), https://studentprivacymatters.org/tag/zoom-third-party-tracking/ [https://perma.cc/UN86-RRFW].

87. *See id.*

Consider the following example of Google's overlapping functions in school settings:

> It's not at all unusual for students to enter one of G Suite's educational services through their student accounts, then venture out from there to one of Google's commercial services, like Maps or Search. For years, Google has declined to provide detailed answers to questions about exactly how it collects and uses information generated by students in those circumstances–making it difficult for schools to determine for COPPA purposes whether G Suite is strictly for the benefit of schools and students within the 'educational context.'[88]

Although Google offers educational services for students, it is easy for students to flip between Google's educational and commercial services, which creates questions of how students' information gets collected and used.[89] Even though students appear to be protected from website operators that collect children's personal information for commercial purposes, uncertainty arises when websites and services that are not purely educational are used for educational purposes, such

88. *See* Herold, *supra* note 11.

89. *See* Natasha Singer, *How Google Took Over the Classroom*, N.Y. TIMES (May 13, 2017), https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html [https://perma.cc/R9GK-4YHU]. Confusion over how student information is being collected by platforms like Google is problematic because "[u]nlike Apple or Microsoft, which make money primarily by selling devices or software services, Google derives most of its revenue from online advertising—much of it targeted through sophisticated use of people's data." *Id.* Students may therefore be using services like Google for educational purposes while Google is collecting student data for commercial purposes. *See id.*

as some of Google's services.[90] As a result, "the lines of COPPA compliance become blurred."[91]

D. COPPA and Teenage Students

Because COPPA only applies to children under thirteen, the rule's protections do not include teenage students using educational technologies at the direction of their institutions.[92] COPPA's critics recognize that "teenagers are vulnerable to information misuse, sometimes even more so than young children."[93] For one, teenagers' online vulnerability may stem from their increased susceptibility to targeted advertisements that prey on their "psychological weaknesses."[94] Yet websites and services directed toward teenagers are not subject to COPPA enforcement.[95]

Recognizing this limitation, COPPA critics believe that "[t]he Children's Online Privacy Protection Act is long overdue for improvements to protect the rights of older teens who spend so much time on mobile and online platforms but who aren't always savvy

---

90. *See* Kiesecker, *supra* note 86; Singer & Conger, *supra* note 38. The uncertainty of determining whether technologies have educational or commercial purposes in schools is particularly concerning considering Google's reach in classrooms across the country. The following demonstrates Google's influence:

> Today, more than half the nation's primary- and secondary-school students—more than [thirty] million children—use Google education apps like Gmail and Docs, the company said. And Chromebooks, Google-powered laptops that initially struggled to find a purpose, are now a powerhouse in America's schools. Today they account for more than half the mobile devices shipped to schools.

Singer, *supra* note 89.

91. Peddy, *supra* note 19, at 139.

92. *See generally* 15 U.S.C. § 6501; *Complying with COPPA*, *supra* note 8 ("Although COPPA does not apply to teenagers, the FTC is concerned about teen privacy and does believe that strong, more flexible, protections *may* be appropriate for this age group.") (emphasis added).

93. Matecki, *supra* note 9, at 389. Matecki explains teenage vulnerability in the context of Internet privacy issues:

> The expanded abuse of young people's personal information, along with other dangers from over-sharing online since COPPA's enactment, have proven that such vulnerabilities are not limited to young people under thirteen. Given the social pressures teens face to interact online, . . . it is no longer accurate to assume that teenagers are protected from the risks of dissemination of personal information online.

Id. at 399–400.

94. *Id.* at 390.

95. *Id.* at 389.

enough to protect themselves from deceptive online ads and digital manipulation."[96] But amending COPPA to include teenagers is unlikely to resolve the underlying issues with COPPA's application to students; the complications arising from the third-party tracking problem, and the inability to distinguish if a technology has purely educational or commercial purposes, makes an amendment raising the age requirement unworkable.

Regardless, the COVID-19 pandemic created a rush to online schooling without careful or advanced planning, and most schools made distance learning websites and technologies mandatory for students.[97] Thus, teenage students essentially had no choice but to use the required education technology, despite the COPPA framework not applying to teenagers (and even if it did, the protections would not have been effective to begin with because of weak enforcement by the FTC).[98] Ultimately, the COVID-19 pandemic has highlighted already-existing inadequacies with COPPA's enforceability, painting a clearer picture for why federal online privacy laws need reworking to protect students when they use educational technologies.

---

96. Rachel Lerman, *New Bill Would Update Decades-Old Law Governing Children's Privacy Online, Add Protection for Teens*, WASH. POST (July 29, 2021, 4:52 PM), https://www.washingtonpost.com/technology/2021/07/29/coppa-update-teenagers-online/ [https://perma.cc/3M8K-PT4F] (statement of Linda Sherry, Director of National Priorities, Consumer Action). On May 13, 2021, Senators Edward Markey and Bill Cassidy introduced the Children and Teens' Online Privacy Protection Act that amends COPPA to protect children ages thirteen to fifteen. Children's and Teens' Online Privacy Protection Act, S. 1628, 117th Cong. (2021); Hunton Andrews Kurth's Privacy & Cybersecurity, *Senate Bill Would Expand Federal Children's Privacy* Protections, NAT'L L. REV. (May 12, 2021), https://www.natlawreview.com/article/senate-bill-would-expand-federal-children-s-privacy-protections [https://perma.cc/5HJY-EQBZ].

97. Keene, *supra* note 49; Li, *supra* note 66, at 1706–07 ("Students learning online have to accept the privacy practices of every remote technology that schools insist on using. While some of these education sites and apps may have strong privacy protections in place, many do not." (citations omitted)); Butler & Zhou, *supra* note 60, at 1614 ("Students do not have a choice but to 'Zoom-in,' . . . and smile for the camera."); Li, *supra* note 51, at 859 (Li explains that the COVID-19 public health emergency led to the "deployment of privacy-invasive technologies and technologically influenced programs" and people "have been asked to accept more and more privacy-violating technologies."). Li describes the pandemic's effects on privacy rights:

> The pandemic forced millions around the world to experience the effects of context collapse, as we faced the slow blurring of the boundaries between previously segmented social spaces, like work, school, home, and more. . . . Students lost the educational privacy afforded to them by the physical space of schools and universities.

Id. at 858.

98. *See* Keene, *supra* note 49.

III. PROPOSAL

After recognizing COPPA's inadequacies and shortcomings in light of the COVID-19 pandemic, legal scholars offered recommendations for addressing growing Internet privacy concerns. These recommendations, however, must consider the challenges of regulating not only the Internet's expansiveness but also legislating in an area already complicated by a web of privacy laws.[99] Despite the apparent challenges, improving young people's privacy on the Internet is still an attainable goal.[100] We can acknowledge that COPPA is antiquated and still "revisit its objectives and offer a fresh approach that is better adapted to today's society and digital landscape."[101]

A. Existing Recommendations for Addressing Internet Privacy Concerns

One suggested approach is to strengthen the privacy laws that are already in existence.[102] This measure would involve strengthening or amending the COPPA statute to better address online privacy concerns. A common suggestion is to make age-related amendments to COPPA that would eliminate age specifications and give protections to all website users regardless of age.[103] The idea is that "the fundamental failure of COPPA is that its applicability is contingent

99. *See* Matecki, *supra* note 9, at 399. There are "challenges of drafting effective legislation to regulate the Internet, especially given its expansive nature." *Id.*; Li, *supra* note 51, at 860 ("It is difficult to grasp the full landscape of privacy in pandemic, due to the ever-expanding web of laws and regulations that touch upon privacy and technology.").

100. *See* Stephen Beemsterboer, *COPPA Killed the Video Star: How the YouTube Settlement Shows that COPPA Does More Harm Than Good*, 25 ILL. BUS. L.J. 63, 83 (2020) ("[T]his is not to say that children's privacy on the [I]nternet is an unattainable goal.").

101. *Id.*; O'Donnell, *supra* note 9, at 495 ("Both the VPPA and COPPA are antiquated; however, both can be fixed.").

102. *See, e.g.*, Li, *supra* note 66, at 1715.

103. *See* Matecki, *supra* note 9, at 398 ("Some commentators have suggested that an overhaul of COPPA that eliminates age distinctions and parental consent requirements would be the most effective means of revision. . . ."); *see also* Beemsterboer, *supra* note 100 ("Congress should adopt [I]nternet privacy regulations that apply protections to all users regardless of age.").

upon age."[104] Making age-related amendments to COPPA seems like an attractive solution; however, the approach faces criticism. For one, removing COPPA's age distinction goes against the legislative intent to protect children under thirteen who are deemed generally incapable of making Internet privacy decisions without parental consent.[105] Regardless, simply removing age distinctions in the COPPA statute while making no other changes is not likely to lead to any significant changes in privacy protections as long as the FTC continues to enforce COPPA weakly and produce unimpressive settlements.

That being said, improving COPPA may require adjusting the FTC's enforcement and settlement policies, which is not a COPPA amendment at all.[106] A stronger enforcement measure could involve setting the penalty for violating COPPA as a percentage of the company's income, like in the European Union where regulators set damages at 4% of the violating company's income.[107] This measure creates a penalty that monetarily affects companies violating COPPA, as opposed to having companies pay an arguably insignificant penalty that does little to deter COPPA violations.[108] Addressing COPPA's underlying enforcement issues may better protect data privacy in the long run.

Additionally, with the recognition that "rights to educational privacy are limited," some commentators recommend "creating a right to educational privacy" because COPPA's protections are simply not

104. Beemsterboer, *supra* note 100.

105. Matecki, *supra* note 9, at 398 ("[W]hile a revision to COPPA eliminating all age barriers would address the problematic concept of parental consent, it ignores the particular vulnerabilities of children and adolescents and, as such, would push aside the original legislative intent of COPPA regulations.").

106. O'Donnell, *supra* note 9, at 495 ("[I]t follows that the area that needs the most attention might not be in COPPA itself; instead, the FTC's settlement policy needs to change. FTC settlements need to monetarily impact the companies charged with violating COPPA."); Kimberly Dempsey Booher & Martin B. Robins, *American Privacy Law at the Dawn of a New Decade (And the CCPA and COVID-19): Overview and Practitioner Critique*, 24 MARQ. INTELL. PROP. L. REV. 169, 199 (2020). But "[w]hile it is appropriate for the FTC to demonstrate that the [COPPA] statute is not a dead letter by going after those who blatantly disregard its existence, this will not suffice." *Id.* (citations omitted).

107. O'Donnell, *supra* note 9, at 495–96.

108. *See id.* at 495; *see also What's Going on with the Children's Online Privacy Protection Act (COPPA)?*, *supra* note 9 ("If you fine the local bakery a million dollars, it's dead. If you fine Google a million dollars, does it deter them from misbehaving in the future? They can pay that fine over and over without having to restructure a thing.").

enough.[109] This measure suggests leaving COPPA intact and enacting a separate educational privacy law for students.[110] Although creating a separate right to educational privacy may appear to accomplish the goal of protecting students in educational settings who use virtual learning technologies, another privacy law that is similar to COPPA may face similar enforcement challenges. Given the continuing issue of the FTC weakly enforcing the existing COPPA statute, there is no guarantee that a separate statute protecting the privacy rights of students would be enforced to any significant degree under the FTC's authority.[111] Simply creating a statute similar to COPPA, but for students in educational settings, would not fully prevent the unauthorized collection and use of student data.

Another recommendation that goes beyond amending the COPPA statute is to create a separate statute that serves as an absolute prohibition on website operators collecting information for commercial purposes in certain environments.[112] An absolute prohibition would prevent the collection of personal data or information even if parental consent is obtained, which in turn creates an absolute protection that can be consistently applied.[113] This approach claims to "eliminate[] any of the previous confusion caused by the need to obtain 'verifiable parental consent'" and "prevent both inconsistent interpretation and potential violations of student

109. Li, *supra* note 66, at 1707, 1716; *What is FERPA?* U.S. DEP'T OF EDUC.: PROTECTING STUDENT PRIV., https://studentprivacy.ed.gov/faq/what-ferpa [https://perma.cc/UT2Z-CWS2]. The Family Educational Rights and Privacy Act (FERPA), although technically an education privacy statute, is a federal law that gives "parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosures of personally identifiable information from the education records." *Id. See generally* 20 U.S.C. § 1232(g) (FERPA statute); 34 C.F.R. § 99 (2022) (FERPA regulations). FERPA thus primarily deals with education records as opposed to students using educational technologies at school or in distance learning environments. *See generally* § 1232(g); § 99.

110. *See* Li, *supra* note 66, at 1716.

111. *See* O'Donnell, *supra* note 9.

112. Peddy, *supra* note 19, at 154. The author suggests using the following language as an absolute prohibition on collecting student data: "In a K-12 institution, no operator shall knowingly engage in targeted advertising, sell a student's information, or use a student's personal information for any purpose other than the educational purpose for which the operator was contracted, unless disclosure is made for reasons required by law or court order." *Id.* (citations omitted).

113. *Id.* at 154–55.

privacy."[114] Yet it is difficult to determine from the outset if a statute would completely eliminate confusion and be entirely straightforward in its application. Any statute, even one labeled as an "absolute prohibition," could lend itself to different interpretations and inconsistencies in application. Thus, a statute removing the parental consent requirement and completely prohibiting online data collection from children would not be sufficient by itself to resolve Internet privacy concerns.

B. The European Union's Approach to Data Protection and Online Privacy

A final existing recommendation to improve Internet privacy protections is for the legislature to pass a federal privacy law.[115] Currently, there is "no single federal law" that regulates online privacy.[116] A federal privacy law that reaches beyond just protecting children under thirteen would serve to "create a national framework for thinking about privacy instead of relying on a patchwork of sectoral privacy laws that do not reflect the realities of privacy today."[117] This type of overarching federal privacy law mirrors online privacy standards set forth in the European Union.[118]

The EU General Data Protection Regulation ("GDPR") is a law that regulates how personal data can be processed and transferred, and its

---

114. *Id.*; *A Four-Step Beginner's Guide to COPPA Compliance*, TWO HAT (Aug. 23, 2017), https://www.twohat.com/blog/beginners-guide-coppa-compliance/ [https://perma.cc/2DBH-DQTB]. There is a general consensus that COPPA is difficult to fully understand, with commentators noting that COPPA is a "large and complex rule" and it "can be confusing to navigate." *Id.*; Sullivan, *supra* note 74 ("COPPA compliance requirements can be unclear.").

115. Li, *supra* note 66, at 1714; Li, *supra* note 51, at 860 ("[I]t is past time for Congress to pass a national privacy law that would provide cohesive, coherent rules based on core privacy values, that could then be translated to different sectors, industries, types of data, and types of data actors."); Butler & Zhou, *supra* note 60, at 1626–27 ("Over the last few years there has been significant interest in Congress establishing a comprehensive data protection framework, but Congress has not yet succeeded in passing such a law.").

116. *Internet Privacy Laws Revealed*, *supra* note 1; Butler & Zhou, *supra* note 60, at 1623 ("Unlike most other developed countries, the United States does not have . . . any entity singularly charged with overseeing business practices that impact user data."); *Data Privacy Laws: What You Need to Know in 2022*, OSANO (June 24, 2020), https://www.osano.com/articles/data-privacy-laws [https://perma.cc/UW9N-MXE7].

117. Li, *supra* note 66, at 1714.

118. *Id.* at 1714–15.

applicability is relatively broad in scope.[119] The GDPR is the source of the provision that sets noncompliance fines at 4% of the company's annual revenue if the company violates the law.[120] Ultimately, the GDPR requires that "whenever information directly or indirectly identifying you as an individual is stored or processed, your data protection rights have to be respected."[121] The GDPR serves as an all-encompassing protection against the collection and use of online personal information.

Because the GDPR offers broad protections, "most consumers are pleased with the precedent of data protection that the GDPR has set."[122] Compared to the FTC's weak enforcement of COPPA, in the first year of GDPR's enforcement, there were 144,000 complaints filed with GDPR enforcement agencies and $63 million in fines issued.[123] Google also faced a $57 million fee for noncompliance under the GDPR for its data harvesting practices.[124] Companies that fail to comply with GDPR's requirements are subject to these penalties and large fines.[125] Currently, online privacy enforcement procedures in the United States are nowhere near GDPR enforcement levels.

---

119. *European Union–Data Privacy and Protection*, INT'L TRADE ADMIN., https://www.trade.gov/european-union-data-privacy-and-protection [https://perma.cc/CK8X-TCV2].

120. *Id.*

121. *Data Protection and Online Privacy*, YOUR EUR., https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm [https://perma.cc/72JV-EKUN] (July 1, 2022).

122. Rob Sobers, *A Year in the Life of the GDPR: Must-Know Stats and Takeaways*, VARONIS: INSIDE OUT SEC. BLOG, https://www.varonis.com/blog/gdpr-effect-review/ [https://perma.cc/EYQ3-2JUQ] (June 17, 2020).

123. *Id.* If there is a confirmed GDPR violation, fines are levied against the offending company in the following way:

> If there is a less serious violation the administrative fines can go up to 10 000 000 EUR (10 million euro), or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In case of more serious violations this goes up to 20 000 000 EUR (20 million euro) or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. These fines are substantial and can financially cripple companies and even put some companies out of business. It is therefore important to fulfill the obligations under the GDPR.

Alex Tolsma, *GDPR Top Ten #7: Data Protection Authority Enforcement Methods*, DELOITTE, https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-data-protection-authority-enforcement-methods.html [https://perma.cc/UG47-2CNP].

124. Sobers, *supra* note 122.

125. *Id.*

The GDPR does, however, include specific rules for children that are similar to COPPA's requirements.[126] Parental approval is required for children to access online services that use children's personal data, but parental consent is no longer required once the child is sixteen years old (in some EU countries) as opposed to thirteen years old in the United States.[127] More notable is the fact that the EU created a privacy law across all EU countries that includes a subset of specific rules applicable only to children. And because COPPA critics are especially concerned with privacy rights for students using educational technologies in a COVID-19 pandemic world, creating a comprehensive federal privacy law in the United States that also provides specific rules for students becomes an attractive option.

C. The Solution: A Federal Privacy Law with Narrower Rules for Students Using Educational Technologies

The GDPR is an excellent privacy law model for the United States, both in the types of conduct that the GDPR protects and in how the GDPR is enforced. In comparison, "COPPA is a relatively 'short & sweet' piece of US legislation covering a handful of distinct areas. GDPR looks very different. . . . [I]t provides a complete security and protection framework for the processing of EU residents' data—both

126. *Data Protection and Online Privacy*, *supra* note 121. On its website, the UK's Information Commissioner's Office provides guidance for organizations that process children's personal data that focuses on the "additional, child specific considerations" of the GDPR. *Children and the UK GDPR, About This Guidance*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/ [https://perma.cc/BGJ9-JZMA]. This is because the "UK GDPR contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in plain clear language that they can understand." *Id.* Recital 38 of the UK GDPR explains the reasoning behind children receiving specific protections:

> Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

Children and the UK GDPR, What Should Our General Approach to Processing Children's Personal Data Be?, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be/ [https://perma.cc/3AFY-P5L9].

127. *Data Protection and Online Privacy*, *supra* note 121.

online and offline."[128] A privacy law viewed as "short and sweet" can hardly be said to offer the same level of data privacy protections as a more comprehensive federal privacy law such as the GDPR. To be consistent with foreign privacy protection standards, the United States should adopt a federal privacy law that includes specific rules protecting children under thirteen as well as specific rules protecting students using educational technologies.

But because the FTC has jurisdiction over commercial entities under its authority to prevent unfair or deceptive trade practices, we arrive at the same issue of FTC enforcement.[129] Before a federal privacy law can be effective, additional measures need to be taken to ensure that the law will be sufficiently enforced. On the bright side, the FTC seemed to be aware (even before the COVID-19 pandemic) that changes in privacy law were needed.[130] This is evidenced by the fact that the FTC began conducting its ten-year review of COPPA four years ahead of schedule back in 2019.[131] If the FTC addresses widespread support for stricter COPPA enforcement, this could encourage the FTC to administer harsher penalties if a federal privacy law is enacted.

If enforcement issues are addressed and resolved, a federal privacy law modeled after the GDPR that offers widespread Internet privacy protections in addition to special rules for children and students would offer the best protections for these groups. Similarly, the GDPR already includes rules specific to children using websites and technologies: "If your product or service offering is squarely child-focused, there are specific child-related provisions to follow (relating to consent, for instance). But at the same time, you'll need to get to grips with all aspects of GDPR."[132] Website operators are not only required to comply with the GDPR's child-related provisions but

128. Archie Stephens, *The Relationship Between COPPA and GDPR: Getting it Right for Your Business*, PRIV. COMPLIANCE HUB (June 2018), https://www.privacycompliancehub.com/gdpr-resources/the-relationship-between-coppa-and-gdpr-getting-it-right-for-your-business/ [https://perma.cc/GSA7-AZGF].

129. *Data Privacy Laws: What You Need to Know in 2022*, *supra* note 116.

130. *See* O'Donnell, *supra* note 9, at 495.

131. *Id.*; Murphy et al., *supra* note 42; Fair, *supra* note 44.

132. Stephens, *supra* note 128.

also with the entirety of the GDPR rules and requirements. Following this framework, a federal privacy law in the United States couldshould require website and service operators to comply with student-related provisions of the statute in addition to overarching federal privacy laws. This way, students using educational technologies in a school setting or at the direction of their instructions will be offered an additional layer of protection that goes beyond current COPPA protections.

CONCLUSION

Congress enacted COPPA to prevent young children's personal information from ending up in the wrong hands. By requiring parental consent before website operators could collect personal information from children under thirteen years old, the aim was to give parents more control to protect their children's information online.[133] Despite the goal of increasing parental involvement, COPPA protections do not apply in school settings.[134] So, in practice, teachers and administrators are requiring students to use websites and technologies that collect and distribute student information without parental consent, which is precisely the type of conduct that COPPA protections seek to avoid. The existing problem has only been exacerbated by the COVID-19 pandemic because the rush to conduct online school led to a steep increase in students of all ages using educational technologies.[135] The recent cybersecurity concerns emerging from life online are bringing attention to defects in the United States' outdated privacy laws. Although a comprehensive federal privacy law modeled after the European Union's GDPR could offer more expansive online privacy protections, the FTC's weak enforcement of existing privacy statutes places this goal slightly out of reach. Yet the increase in conversations in the legal community

133. *See Complying with COPPA*, *supra* note 8.
134. *Id.*
135. *See* Keene, *supra* note 49.

regarding post-pandemic cybersecurity concerns may very well lead to stricter enforcement of online privacy laws in the near future.