NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
14 N.C. J.L. & TECH. ON. 167 (2013)

CHILDREN'S PRIVACY IN VIRTUAL K–12 EDUCATION: VIRTUAL SOLUTIONS OF THE AMENDED CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA) RULE

David R. Hostetler* & ***Seiko F. Okada*****

Virtual K–12 education, roughly defined as electronically-mediated teaching and learning for children, has expanded dramatically in the past decade. In December 2012, the Federal Trade Commission approved its first amendments to its original Rule implementing the Children's Online Privacy Protection Act. These changes aim to strengthen the regulation over website operators and application developers to collect personal information from children under thirteen with verifiable parental consent. The amended Rule, however, will likely only offer "virtual" solutions to problems of children's online privacy threats. The amended Rule fails, for instance, to clarify educators' roles and responsibilities as parental surrogates in protecting children's privacy in virtual education—an issue identified as early as the original implementation of the Children's Online Privacy Protection Act. This article considers some of the existing realities and vulnerabilities of children engaged in virtual education and potential legal problems, as well as proposed solutions.

I. INTRODUCTION

The Children's Online Privacy Protection Act ("COPPA") was enacted in 1998 to protect children's online safety.[1] The Federal

* Associate Professor of Law, Education, and Leadership Studies, Appalachian State University, Boone, North Carolina. Hostetler has taught and practiced education law since 1994. He previously served thirteen years as Legal Director for the University of North Carolina Principals' Executive Program. He is a graduate of Duke University (J.D., M.A. in Political Science, 1990), Gordon-Conwell Theological Seminary (M.A.T.S., 1987), and Westminster College (B.A., 1983).

Trade Commission ("FTC") enacted regulations implementing COPPA (the "COPPA Rule" or the "Rule") in 1999.[2] Children's Internet use has dramatically increased since then, especially with the rise of social networking sites and mobile Internet devices.[3] Responding to the increased use of the Internet by children in the mobile and social networking era, the FTC amended the COPPA Rule on December 19, 2012.[4] The amended Rule, effective July 1, 2013,[5] strengthens regulation over website operators and by expanding COPPA's reach to mobile application developers and third-party vendors in prohibiting the collection of personal information from children under thirteen without verifiable parental consent.[6] The amended Rule aims to "strike the right balance between protecting innovation that will provide rich and

---

** J.D. Candidate, University of North Carolina, 2014. Ph.D. in Medical Sciences (Cell Biology), M.D., University of Tokyo. Okada has served in the field of children's law, including internships at Child's Advocate as well as the North Carolina Division of Child Development and Early Education. The authors thank Ms. Barbara Herrera for her insightful guidance.

[1] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, §§ 1301–1308, 112 Stat. 2681–2728, 2681-728 to 2681-735 (codified at 15 U.S.C. §§ 6501–6506 (2006)). COPPA should be distinguished from the Children's Online Protection Act ("COPA"). *See* 47 U.S.C. § 231 (2006). COPA sought to restrict minors' access to sexually explicit materials on the Internet. *See id.* COPA has been held unconstitutional on the First Amendment grounds. *See* Ashcroft v. ACLU, 542 U.S. 656, 672–73 (2004); ACLU v. Mukasey, 534 F.3d 181, 207 (3d Cir. 2008).

[2] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (to be codified at 16 C.F.R. pt. 312). The COPPA Rule was issued on October 21, 1999 and took effect on April 21, 2000. *Id.* The COPPA Rule provides website operators with guidelines on how to comply with COPPA's requirements. *See id.*

[3] *See* 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, 370–71 (2010).

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

[5] *Id.*

[6] *See id.*

engaging content for children, and ensuring that parents are informed and involved in their children's online activities."[7]

With the rapid development of electronic devices and the Internet, teaching and learning at many schools no longer consists solely of face-to-face classroom lectures, whiteboards, textbooks, paper, and pencils. Schools have dramatically expanded their use of computers, Internet resources,[8] and mobile devices[9] to facilitate teaching and learning. All such electronic educational devices, collectively referred to in this article as "virtual education,"[10] are now an important part of most children's education.[11] Contrary to public perception, the law does not provide special privacy protection tailored to virtual education.[12] In virtual education, children are as vulnerable to threats of unauthorized collection and use of their personal information by third parties as they are when

[7] Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information by Amending Children's Online Privacy Protection Rule (Dec. 19, 2012), *available at* http://www.ftc.gov/opa/2012/12/coppa.shtm.

[8] These resources include the viewing of websites and YouTube videos in class, use of educational interactive websites, and use of online homework assistance.

[9] These devices can range from something as small as a smartphone to even an iPad.

[10] This definition applies to this Recent Development article. Others may attach different meanings to the term "virtual education." *See infra* Part II.B.

[11] *See* iNACOL, FAST FACTS ABOUT ONLINE LEARNING 1–2 (2012), *available at* http://www.inacol.org/cms/wp-content/uploads/2012/11/iNACOL_fastfacts_October_2012.pdf (illustrating increasing implementation of online education in the United States).

[12] *See generally* 15 U.S.C. §§ 6501–6506 (2006) (providing no specific provision for virtual education in COPPA); Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312) (providing no specific provision or consideration for virtual education in the amended COPPA Rule); Susan P. Stuart, *Lex-Praxis of Education Informational Privacy for Public Schoolchildren*, 84 NEB. L. REV. 1158, 1158–1225 (2006) (providing no specific statutory provision prohibiting unauthorized access to children's personal information by third parties in virtual education).

using mobile devices and the Internet outside the education context.[13]

The COPPA framework, including the amended Rule, however, fails to give any special attention to children's online privacy threats in virtual education. For example, the amended Rule continues, after more than a dozen years, in failing to define the role of school officials acting as parental surrogates in providing consent for children's information being collected by website operators and mobile application ("app") developers.[14] The definition of "school officials" in this context is also unclear.[15] The amended Rule also leaves unclear whether parental consent is waived when educational websites and apps collect data for limited purposes of internal school use.[16]

This Recent Development analyzes the gap between the emerging issues of children's online privacy threats in virtual education and the COPPA framework that was updated by the 2012 amended Rule and suggests possible regulatory changes to better protect children's online privacy without unreasonably inhibiting children's access to useful virtual learning opportunities. Part II reviews the evolution of the Internet technology including the recent rise of virtual K–12 education. Part III reviews implementation of the COPPA and the COPPA Rule in 1998 and 1999, respectively, and the long-awaited amendment to the COPPA Rule in 2012. Part IV analyzes legal and practical issues of children's privacy in virtual education that are not addressed by COPPA or the amended COPPA Rule. Finally, Part V advocates for new law and policy that protects children's online privacy in virtual education without unreasonably preventing children from benefiting from virtual education resources.

---

[13] Children may be *more* vulnerable to online privacy threats in virtual education at school than at other settings, because at school parents are not immediately available to review privacy statements of websites and serve as gatekeepers. *See infra* Part II.B.

[14] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. at 3972.

[15] *See id.*

[16] *See id.*

II. EVOLUTION OF INTERNET TECHNOLOGY AND VIRTUAL EDUCATION

This Part reviews recent advances of Internet technology in virtual education, as well as privacy threats to children created by such advances.

A. *Increased Use of Internet Technology by Children*

Since the mid-1990s, the Internet, with the rise of the World Wide Web and e-mail, has had a revolutionary impact on communication and commerce.[17] The number of Internet users has grown extensively since this time.[18] Children have represented a large segment of online consumers.[19] In 1997, "almost 10 million, or fourteen percent, of America's 69 million children were online, with over 4 million accessing the Internet from school and 5.7 million from home."[20] Third parties, including website operators, advertisers, and market researchers, have been able to collect Internet users' personal information and compile user profiles with identifying information.[21] The architecture of the Internet even allows third parties to closely track an individual's browsing

[17] *See Imagining the Internet: A History and Forecast*, ELON UNIV. SCH. OF COMMC'NS, http://www.elon.edu/e-web/predictions/150/1960.xhtml?m=1 (last visited Mar. 16, 2013).

[18] *See id.* ("In 1996, there were approximately 45 million people using the Internet. By 1999, the number of worldwide Internet users reached 150 million, and more than half of them were from the United States. In 2000, there were 407 million users worldwide. By 2004, there were between 600 and 800 million users . . . ."); *see also* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 3 (1998) ("By December 1997, the number of adults online in the U.S. and Canada had climbed to 58 million, and 10 million had actually purchased a product or service online. Analysts estimate that Internet advertising—which totaled approximately $301 million in 1996—will swell to $4.35 billion by the year 2000." (internal citations omitted)).

[19] FED. TRADE COMM'N, *supra* note 18, at 4.

[20] *Id.*

[21] Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J. L. SCI. & TECH. 281, 282 (2012) ("Every search, query, click, page view, and link are logged, retained, analyzed, and used by a host of third parties . . . .").

activities on the Internet ("online behavioral tracking"), compile a detailed personal profile, and conduct "online behavioral advertising" that specifically target the individual based on his personal profile.[22] Such online behavioral tracking has created unease for Internet users.[23]

The emergence of social networking sites inaugurated new types of online privacy problems in the 2000s. Facebook and Twitter, for example, were launched in 2004 and 2006, respectively.[24] Since their launch, the social networking sites rapidly became popular among adults and children.[25] In 2012, for example, "7.5 million children under the age of thirteen [had] Facebook accounts, and 5 million of these children [were] under the age of ten."[26]

Children's expansive engagement in social networking sites triggered privacy threats related not only to online tracking and advertising but also to sex crimes.[27] Social networking sites are meant for voluntary sharing of personal information with others.[28]

---

[22] *Id.* at 282–83.

[23] *Id.* at 283–84 & n.8.

[24] *About*, FACEBOOK, https://www.facebook.com/facebook/info (last visited Mar. 16, 2013); Jack Dorsey (@ Jack), TWITTER (MAR. 21, 2006, 12:50 PM), https://twitter.com/jack/status/20 ("just setting up my twttr").

[25] Craig Smith, *(March 2013) How Many People Use the Top Social Media, Apps & Services?*, DIGITAL MKT. RAMBLINGS (Mar. 2, 2013), http://expandedramblings.com/index.php/resource-how-many-people-use-the-top-social-media/ (internal citations omitted). According to a survey of firm reports, Facebook had 1.06 billion monthly active users and more than 50 million pages in 2012; Twitter had 500 million total users and more than 200 million active users in 2012. *See id.* For Facebook's data as of December 31, 2012, *see* Facebook Inc., Annual Report (Form 10-K) 5 (Dec. 31, 2012), *available at* http://files.shareholder.com/downloads/AMDA-NJ5DZ/2301311196x0xS1326801-13-3/1326801/1326801-13-3.pdf.

[26] Julie Brill, *Privacy & Consumer Protection in Social Media*, 90 N.C. L. REV. 1295, 1302 (2012). This was the case even though Facebook's terms of service do not allow children under the age of thirteen to open an account. *Id.*

[27] *See Predators Access to Kids*, ENOUGH IS ENOUGH, http://www.internetsafety101.org/predatorsonline.htm (last visited Mar. 30, 2013).

[28] *See Dangers of the Social Web*, ENOUGH IS ENOUGH, http://www.internetsafety101.org/snsdangers.htm (last visited Mar. 16, 2013).

To that end, social networking sites facilitate a sense of virtual intimacy, where one feels comfortable sharing personal information with a stranger, perhaps more than in a face-to-face interaction.[29] Without proper knowledge of online safety and privacy, children can easily become "friends" with predators and provide them with personal information.[30] Studies have indicated that thirty-three percent of all types of Internet-related sex crimes against minors involved social networking sites.[31]

Another major change in the Internet landscape is the rise of smartphones and apps that have enabled users to use the Internet from personal mobile devices.[32] The market for mobile apps has rapidly expanded from its introduction in 2008.[33] In 2012, consumers, including children, had access from an expansive variety of mobile devices to over "500,000 apps in the Apple App store and 380,000 apps in the Android Market."[34] As of December 31, 2012, Facebook had 680 million mobile users and had more than 10 million apps and websites integrated in the Facebook web pages.[35] New privacy concerns have emerged where mobile apps, for example, can automatically capture user information from a mobile device and share it with third parties.[36] Mobile apps can also capture any data linked or stored on a mobile device, including the

[29] *See id.*

[30] *See id.*

[31] Kimberly J. Mitchell et al., *Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization*, 47 J. ADOLESCENT HEALTH 183, 185 (2010).

[32] *See* FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING 1 (2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf (illustrating the increased use of mobile devices and apps).

[33] *Id.*

[34] *Id.* (footnotes omitted).

[35] *See* Facebook Inc., *supra* note 25, at 5–6. Development of the Facebook Platform, "a set of development tools and application programming . . . interfaces that enables developers to easily integrate with Facebook to create . . . apps and websites," promoted integration of such a large number of apps and websites into the Facebook pages. *Id.* at 6.

[36] *See* FED. TRADE COMM'N, *supra* note 32, at 1.

user's geolocation, phone number, call logs, contacts, calendars, and unique device identifiers.[37]

In sum, recent advances in Internet technology, including social networking sites and mobile apps, pose high levels of privacy threats to child users.

B. *Evolution of Virtual Education*

The Internet and Internet devices have and will continue to revolutionize the delivery and substance of education.[38] Virtual education is broadly defined here as any teaching and learning that is conveyed, either wholly or in part, by electronic interactions of teachers and students and student exposure to learning resources via electronic means using the Internet.[39] Virtual education is mediated by various technologies and can be "either comprehensive or supplementary to a child's education."[40] Proponents of virtual education point to advantages such as flexibility in time and location, increased access to higher-quality teachers and resources, improved student productivity, and decreased costs, as compared to conventional face-to-face education.[41]

In November 2009, forty-five states and the District of Columbia had a state-operated part-time virtual school, a full-time virtual school, or both.[42] A survey in the same year revealed that seventy-five percent of school districts had one or more students participating in some form of online learning.[43] Moreover, sixty-

---

[37] *Id.*

[38] *See* Dan Lips, *How Online Learning Is Revolutionizing K–12 Education and Benefiting Students*, BACKGROUNDER, Jan 2010, at 1, 1–2, *available at* http://s3.amazonaws.com/thf_media/2010/pdf/bg_2356.pdf.

[39] *See id.* at 2–3.

[40] *Id.* Further, virtual education programs can either be publicly-supported as a part of the school education or be accessed independently from the school education. *Id.* This Recent Development focuses on Internet-associated K–12 virtual education offered as part of the school education.

[41] *See id.* at 3–4.

[42] *Id.* at 5. A full-time virtual school provides education exclusively by electronic means and can be operated either by a state or a private entity. *See id.* at 3.

[43] *Id.* at 6.

six percent of school districts expected participation of students in online learning to increase.[44]

Virtual education has progressively integrated new Internet technologies, including mobile apps and social networking websites. In September 2012, "there were approximately 74,000 'education' apps in the iTunes App Store, and 30,000 in the Android market."[45] Approximately sixty percent of these education apps targeted children under the age of thirteen.[46] In February 2013, Apple estimated that it had sold 4.5 million iPads to U.S. educational institutions, a sharp increase from 1.5 million in January 2012.[47] Moreover, a variety of social networking interfaces, including blogs, instant messaging, online photo galleries, podcasts, social bookmarks, and social networks, are now available and being used to enhance classroom education.[48] Children are, therefore, increasingly exposed to privacy threats by educational website operators and educational app developers in K–12 education.

III. THE DEVELOPMENT OF COPPA

The ever-expanding use of Internet technology has raised concerns about online privacy protections for children and

[44] *Id.*

[45] Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 4003 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312).

[46] *Id.*

[47] Christian Zibreg, *Apple Sold Eight Million iPads to Education Institutions Worldwide*, IDOWNLOADBLOG (Feb. 28, 2013), http://www.idownloadblog.com/2013/02/28/ipad-8m-sales-education. Further, Apple's website describes usefulness of iPad in virtual education:

> With iPad, the classroom is always at your fingertips. Right now at the App Store, there are more than 20,000 educational apps for all kinds of learners, teaching them everything from science to sign language. Students can track their assignments, take notes, and study for finals. Teachers can give lessons, monitor progress, and stay organized.

Apple in Education, APPLE, http://www.apple.com/education/ipad/ (last visited Mar. 16, 2013).

[48] *See* JUDY CAMPF & SHARON GALLAGHER, SOCIAL NETWORKING IN THE K–12 CLASSROOM 1 (2008–2009), *available at* http://www.apsva.us/cms/lib2/VA01000586/Centricity/Domain/733/Web2VocabBrochure.pdf.

necessitated legal means of protection. Congress and the FTC responded by implementing COPPA and its Rule.[49] The initial COPPA framework, however, has had to be adapted to developing technologies and problems. This Part reviews the COPPA framework and the long-awaited amendment of the Rule in 2012.

A. *COPPA of 1998 and the COPPA Rule of 1999*

Concerns for children's online privacy emerged soon after the advent of the Internet.[50] In 1998, the FTC noted how "[t]he World Wide Web is an exciting new marketplace for consumers" and "the online consumer market is growing exponentially."[51] The Internet allowed third parties, including website operators, advertisers, and market researchers, to collect Internet users' personal information and compile detailed user profiles.[52] Before 1998, no federal law restricted collection of personal information from children online. A survey by the FTC in 1998 demonstrated that eighty-nine percent of websites for children collected child users' personal data including names, e-mail addresses, postal addresses, phone numbers, fax numbers, and social security numbers.[53] Only twenty-four percent of websites, however, posted privacy statements and only one percent required proof of parental consent for a child to use the website.[54] Congress enacted COPPA on October 21, 1998[55] to

[49] *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, §§ 1301–1308, 112 Stat. 2681–2728, 2681-728 to 2681-735 (codified at 15 U.S.C. §§ 6501–6506 (2006)); 16 C.F.R. pt. 312 (2006).

[50] *See generally* FED. TRADE COMM'N, *supra* note 18 (noting that website operators did not post privacy disclosures and yet collected user information); *supra* Part II.A.

[51] FED TRADE COMM'N, *supra* note 18, at i.

[52] *See supra* text accompanying notes 21–23.

[53] *See* FED. TRADE COMM'N, *supra* note 18, at 31–32. The survey demonstrated that 96% of the sites that collected personal information collected an e-mail address, 74% collected a name, 49% collected a postal address, 24% collected a phone number, and 1% collected a social security number. *Id.*

[54] *See id.* at 35–37.

[55] *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, §§ 1301–1308, 112 Stat. 2681–2728, 2681-728 to 2681-735 (codified at 15 U.S.C. §§ 6501–6506 (2006)). COPPA took effect on April 21, 1999. *See id.* at § 1308, 112 Stat. at 2681-735.

address children's privacy concerns identified, in part, by the FTC's 1998 survey.[56] The FTC issued the rule that implemented COPPA on October 21, 1999.[57]

As explained further below, the principal "short-hand" requirements of COPPA involve: (1) "notice" of personal information capture; (2) obtaining "parental consent;" (3) rights of "parental review" of information-gathering practices; (4) prohibiting unconditional collection of personal information; and (5) imposing certain "security" measures.[58]

COPPA prohibits commercial website operators from intentionally collecting personal information[59] from children under the age of thirteen except when: (1) the website operator provides proper notice to website users of the personal information to be collected and (2) the operator obtains verifiable consent from one of the child's parents that authorizes the operator to collect such information.[60] "Verifiable parental consent" means any reasonable effort, using "available technology," and includes a request for authorization for future collection, use, and disclosure described in

[56] *See* Dorothy A. Hertzel, Note, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 FED. COMM. L.J. 429, 437 (2000) (noting that the goals of COPPA are "to enhance parental involvement in a child's activities online, protect the safety of a child while participating in online locations such as chat rooms, secure a child's personally identifiable information collected online, and limit information collection from a child absent parental consent").

[57] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888 (Nov. 3, 1999) (to be codified at 16 C.F.R. pt. 312). The COPPA Rule took effect on April 21, 2000. *Id.*

[58] *See* 15 U.S.C. § 6502; Melanie L. Hersh, Note, *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, 1855 (2001) (citing Laurel Jamtgaard, *Big Bird Meets Big Brother: A Look at the Children's Online Privacy Protection Act*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 385, 388 (2000)).

[59] Personal information includes such things as the child's name, postal address, e-mail address, telephone number, social security number, and personal preferences. *See* 15 U.S.C. § 6501.

[60] *Id.* § 6502(b)(1)(A).

the notice.[61] Further, COPPA requires operators to provide a parent, upon request, with a specific description of personal information collected from a child, a reasonable means to obtain the collected personal information, and an opportunity to refuse the operator's further use of the personal information (the requirement (3) above),[62] prohibits operators of websites from "conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate" (the requirement (4) above),[63] and requires operators to establish procedures that will best protect the collected information (the requirement (5) above).[64] The FTC may impose civil penalties for COPPA violations under the Federal Trade Commission Act.[65] A state may also bring civil actions against COPPA violators.[66]

B. *Initial Effect of COPPA*

COPPA initially proved successful in accomplishing its objectives, though to a limited degree. The FTC conducted a compliance survey in April 2001, a year after implementation of the COPPA Rule.[67] The survey revealed that a majority of the sites directed at children complied with some, but not all, of the requirements of the Rule.[68] Among 144 children's websites that were surveyed, 104 sites (72%) collected personal information,[69]

[61] *Id.* § 6501(9).
[62] *Id.* § 6502(b)(1)(B).
[63] *Id.* § 6502(b)(1)(C).
[64] *Id.* § 6502(b)(1)(D).
[65] *Id.* § 6502(c). The relevant provision of the Federal Trade Commission Act is 15 U.S.C. § 57a(a)(1)(B). *See id.*
[66] *Id.* § 6504.
[67] FED. TRADE COMM'N, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE (2002).
[68] *See id.* at i–ii.
[69] *Id.* at 3. The survey further demonstrated that 85% of the sites that collected personal information collected an e-mail address (as compared to 96% in 1998), 63% collected a name (as compared to 74% in 1998), 14% collected a postal address (as compared to 49% in 1998), 9% collected a phone number (as compared to 24% in 1998), and none collected a social security number (as opposed to 1% in 1998). *Compare id.* (noting statistics in a 2002 survey) *with*

showing a decrease from 89% observed in the 1998 survey.[70] Among sites that collected personal information, 89% provided a privacy policy[71] (as compared to 24% in 1998[72]), and 47% asked for parental consent before collecting children's information[73] (as compared to 1% in 1998).[74] The types and amounts of information collected by websites in 2001 were more limited than those in 1998, suggesting a heightened awareness of online safety and privacy concerns.[75] At the same time, however, only half of the websites complied with COPPA's unconditional collection and parental review requirements.[76] Overall, the survey demonstrated a positive effect of COPPA and the Rule in substantially reducing the incidents of parentally-unapproved collection and use of children's personal information.

C. *Keeping the COPPA Rule Intact*

COPPA required that the FTC review the COPPA Rule within five years of its effective date of April 21, 2000.[77] In 2006, after receiving 116 comments[78] and conducting the mandatory review of the Rule,[79] the FTC concluded that "[n]o changes to the Act or

---

FED. TRADE COMM'N, *supra* note 18, at 31–32 (noting statistics in a 1998 survey).

[70] *See* FED. TRADE COMM'N, *supra* note 18, at 31–32.

[71] FED. TRADE COMM'N, *supra* note 67, at 7. The policy stated whether the site collected personal information, how the information was used, and whether the information was shared with third parties. *Id.* at 8.

[72] FED. TRADE COMM'N, *supra* note 18, at 35.

[73] FED. TRADE COMM'N, *supra* note 67, at 6. Among sites that asked for parental consent, eighty-eight percent asked for a parent's e-mail address, twenty-nine percent provided "print & send" forms. *Id.* Other methods of parental consent included providing a toll-free number and asking for a parent's credit card number. *Id.*

[74] FED. TRADE COMM'N, *supra* note 18, at 37.

[75] *See supra* note 69 and accompanying text.

[76] *See* FED. TRADE COMM'N, *supra* note 67, at 10–11.

[77] *See* 15 U.S.C. § 6506 (2006); 16 C.F.R. § 312.11 (2012).

[78] FED. TRADE COMM'N, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A REPORT TO CONGRESS 7 (2007).

[79] *See* 15 U.S.C. § 6506; 16 C.F.R. § 312.11 (requiring the FTC review the COPPA Rule within five years of its effective date (which is April 21, 2000)).

Rule are necessary at this time."[80] The FTC issued eleven civil penalty actions and "obtained more than $1.8 million in civil penalties" from 2001 to 2006.[81] The FTC believed that such enforcement actions and educational materials promoted website operator compliance with COPPA and the Rule.[82] At the same time, the FTC found that a wide range of child-directed websites remained and that COPPA did not appear to have substantially limited children's ability to access information online.[83] Based on public comments and agency review, the FTC concluded that the COPPA framework was essentially effective in promoting children's online safety while not imposing overly burdensome costs on website operators.[84]

Interestingly, in the same report, the FTC discussed "new and emerging issues in children's online privacy" that are not fully addressed in the COPPA framework created in 1999.[85] For example, the FTC noted a concern regarding social networking sites, stating that "younger children are visiting more general audience websites, such as social networking sites, that are not intended for their use but nonetheless attract their presence."[86] Of particular concern were incidents involving sexual predators' exploitive use of children's personal information acquired from social networking sites.[87] In fact, the FTC noted that it brought and settled its first COPPA violation case involving a social networking site in 2006.[88] The FTC alleged that the operators of Xanga.com collected, maintained, and disclosed personal

[80] FED. TRADE COMM'N, *supra* note 78, at 1.
[81] *Id.* at 16.
[82] *See id.* at 22.
[83] *See id.* at 10.
[84] *See id.* at 10, 27.
[85] *See id.* at 24–28.
[86] *Id.* at 10. The FTC further noted that "there is potential for age falsification on general audience websites, as well as liability under COPPA, should these sites obtain actual knowledge that they are collecting, using, or disclosing personal information from children online." *Id.*
[87] *See id.* at 25.
[88] *See id.* at 26 & tbl.1.

information of 1 million children under thirteen by creating over 1.7 million online child accounts.[89]

The FTC also noted a concern regarding mobile devices, stating that the challenges for the FTC and parents would likely increase as children increasingly used "mobile devices" to access the Internet rather than "stand-alone computers."[90] The FTC, however, concluded that, instead of updating the COPPA framework to adequately address these emerging concerns, it "will closely monitor developments in the market place, and will make recommendations for changes in the Rule, if appropriate."[91]

D. *FTC Recognition of Emerging Privacy Threats*

After foregoing amendments to the COPPA Rule in 2007, the FTC was made aware of emerging privacy threats, escalating in both scope and frequency. In recent years, both the number of COPPA enforcement actions by the FTC and the increasing amount of civil penalties imposed in those actions significantly surpassed those in the preceding years of COPPA implementation.[92] This trend may illustrate two things: the FTC's expanded efforts in COPPA enforcement and increases in the magnitude of COPPA violations. Examples of recent FTC actions against website operators include: (1) a May 2011 action against Playdom, a Disney subsidiary and a leading developer of online multi-player games, for collecting personal information during registration of at least 821,000 children and enabling children to

[89] *See* Complaint at 5–9, United States v. Xanga.com, Inc., No. 06-CIV-6853 (S.D.N.Y. 2006); FED. TRADE COMM'N, *supra* note 78, at 18. Settlement required Xanga's compliance with COPPA and the Rule, deletion of all personal information illegally collected, and a civil penalty of $1 million. *See* Consent Decree at 3–12, *Xanga.com*, No. 06-CIV-6853; FED. TRADE COMM'N, *supra* note 78, at 18.

[90] FED. TRADE COMM'N, *supra* note 78, at 27.

[91] *Id.* at 29.

[92] *See, e.g.*, Complaint, United States v. Artist Arena, No. 12-CV-7386 (S.D.N.Y. 2012), Complaint, United States v. RockYou, Inc., CV-12-1487 (N.D. Cal. 2012), Complaint, United States v. W3 Innovations, LLC, No. CV-11-03958-PSG (N.D. Cal. 2011), and Complaint, United States v. Playdom, Inc., No. SACV 11-00724-AG (C.D. Cal. 2011).

publicly post their full names, e-mail addresses, instant messenger IDs, and location without parental consent,[93] resulting in a $3 million COPPA civil penalty and security enforcement;[94] (2) an April 2012 action against RockYou, a social game site, for collecting personal information from 179,000 children without parental consent and failing to apply reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children,[95] resulting in a $250,000 civil penalty and security enforcement,[96] and; (3) an October 2012 action against Artist Arena, an operator of a group of recording artist websites, for knowingly registering approximately 9,000 children under the age of thirteen for newsletter subscriptions without parental consent,[97] resulting in a $1 million civil penalty and security enforcement.[98]

In August 2011, the FTC launched its first COPPA enforcement action against a mobile application developer.[99] Defendant W3 Innovations develops and distributes mobile apps for the iPhone and iPod Touch that allow users to play games and share information online.[100] The FTC alleged that W3 Innovations collected

[93] *See* Complaint at 6–7, *Playdom, Inc.*, No. SACV 11-00724-AG. Between 2006 and 2010, 403,000 children registered on Playdom's general audience sites and 821,000 children registered on Playdom's Pony Stars children's site. *Id.*

[94] *See* Consent Decree at 6, *Playdom*, No. SACV 11-00724-AG. The $3 million is the largest amount of COPPA civil penalty to date. Jorgen Wouters, *Disney-Owned Company Fined $3 Million for Children's Privacy Violations*, DAILY FIN. (May 13, 2011), http://www.dailyfinance.com/2011/05/13/disney-owned-company-fined-3-million-for-childrens-privacy-vio. Between 2006 and 2010, 403,000 children registered on Playdom's general audience sites and 821,000 children registered on Playdom's Pony Stars children's site. Complaint at 6–7, *Playdom, Inc.*, No. SACV 11-00724-AG.

[95] *See* Complaint at 7–8, *RockYou, Inc.*, No. CV-12-1487. In addition to the COPPA charges, RockYou was charged by the FTC for allowing hackers to access personal information of 32 million users. *Id.* at 4–7.

[96] *See* Consent Decree at 6–10, *RockYou*, No. CV-12-1487.

[97] Complaint at 5, *Artist Arena*, No. 12-CV-7386.

[98] Consent Decree at 3–5, *Artist Arena*, No. 12-CV-7386.

[99] *See* Complaint, United States v. W3 Innovations, LLC, No. CV-11-03958-PSG (N.D. Cal. 2011).

[100] *Id.* at 4.

and maintained over 30,000 e-mails from children and collected, maintained, or disclosed personal information from approximately 600 app users below the age of thirteen without obtaining parental consent.[101] The settlement involved a $50,000 civil penalty and deletion of all illegally-collected data.[102] *W3 Innovations* illustrates a new form of privacy threat linked to mobile use and signifies that mobile app developers, just like website operators, fall within the COPPA regulatory framework.[103]

The FTC also conducted an investigation regarding mobile apps.[104] There are now more than "500,000 apps in the Apple App store and 380,000 apps in the Android Market."[105] The FTC's investigation revealed that practically all mobile apps geared toward children collected personal information with little, if any, disclosures of their data collection and sharing practices to those children or their parents.[106] This was the case even though both Apple and Android app stores require developers by agreement to disclose to users the information the developers' apps collect.[107] As a result of its investigations, the FTC was alerted to the imminent privacy threats to children in their use of the newest Internet technologies.[108]

E. *The 2012 Amended COPPA Rule*

Recognizing the outdated 1998 law had not kept pace with these technological advances,[109] the FTC issued its long-awaited

---

[101] *Id.* at 6–8.

[102] *See* Consent Decree at 4–5, *W3 Innovations*, No. CV-11-03958-PSG.

[103] *See* Complaint at 2, *W3 Innovations*, No. CV-11-03958-PSG (stating that the FTC's complaint states a claim under COPPA).

[104] *See, e.g.*, FED. TRADE COMM'N, *supra* note 32 (investigating app market for children and data collection and sharing practices).

[105] *Id.* at 1 (footnotes omitted).

[106] *See id.* at 12–13.

[107] *Id.* at 12.

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

[109] *See, e.g.*, Matecki, *supra* note 3, at 370 (arguing that COPPA is ineffective in today's Internet landscape and advocating for stricter regulation on collection and dissemination of personal information by websites).

amendments to the COPPA Rule on December 19, 2012.[110] FTC Chairman Jon Leibowitz noted "the rise of smartphones, tablets, social networks, and more than a million apps" and that "while all of these advances have enriched our lives, enhanced educational opportunities, and grown our economy, they also exacerbate the privacy risks to children."[111]

The amended Rule aims to expand the entities and activities regulated by the COPPA framework and to clarify ambiguities that had arisen previously.[112] In short, the amended Rule: (1) expands the definition of "personal information;"[113] (2) expands the definition of "operators" covered by COPPA;[114] (3) expands COPPA coverage to third parties who collect personal information through web operators;[115] (4) redefines existing exemptions to COPPA regulation;[116] (5) redefines methods to obtain verifiable parental consent;[117] (6) strengthens parental notice requirements;[118] (7) requires reasonable procedures to ensure confidentiality and security during data retention and deletion;[119] and (8) strengthens the FTC's oversight of self-regulatory "safe harbor" programs.[120] The amended provisions particularly pertinent to virtual education are discussed below.

---

[110] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. at 3972; Matecki, *supra* note 3, at 370.

[111] Jon Leibowitz, Chairman, Fed. Trade Comm'n, Statement of FTC Chairman Jon Leibowitz on Updated FTC COPPA Rule (as prepared for delivery) 2 (Dec. 19, 2012), *available at* http://www.ftc.gov/speeches/leibowitz/121219coppastmt.pdf.

[112] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. at 3972.

[113] *See id.* at 3978–83, 4009.

[114] *See id.* at 3975–76, 4009.

[115] *See id.* at 3983–84, 4009.

[116] *See id.* at 3992–94, 4011–12.

[117] *See id.* at 3986, 4011–12.

[118] *See id.* at 3984–91, 4010–11.

[119] *See id.* at 3994–95, 4012.

[120] *See id.* at 3992, 4012. "Safe harbor" means that an operator may satisfy the COPPA requirements by following a set of self-regulatory guidelines approved under COPPA. *See* 15 U.S.C. § 6503(a) (2006).

1. *The Definition of "Personal Information"*

The amended Rule has expanded the definition of "personal information" to include "persistent identifiers" linked to a device, geolocation information sufficient to identify a street name and name of a city or town, a photograph, video or audio file containing a child's image or voice, and a screen or user name when it functions as online contact information.[121] Persistent identifiers covered by the amended Rule include those "that can be used to recognize a user over time and across different websites or online services."[122] These include a customer number held in a cookie, an Internet Protocol address, a processor or device serial number, and a unique device identifier.[123] This greatly expands the meaning of "personal information" beyond date of birth, gender, or zip code.[124]

2. *The Definition of an "Operator"*

The amended Rule significantly expands the types of entities covered by COPPA. An "operator" includes a site or service directed at children that integrates outside services, such as plug-ins or advertising networks, that collect personal information from visitors.[125] Consequently, this extends COPPA obligations to operators that do not directly collect personal information from children, but simply allow outside parties to collect such information through plug-ins or advertisements, even if the operators do not have access to or control of information collected by such outside parties.[126] Interestingly, the FTC has specified that mobile platforms, such as Google Play and Apple's App Store, are exempt from this

[121] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. at 4009.
[122] *Id.*
[123] *Id.*
[124] *See id.*
[125] *See id.*
[126] *See id.* at 4009. The FTC notes that an operator benefits from allowing outside parties to collect personal information through its site by direct compensation, enhanced content, or greater publicity gained through social media. *See id.* at 3977. Commissioner Ohlhausen, however, dissented against this provision, stating that the revised definition of an "operator" exceeds the scope of authority delegated by Congress. *See id.* at 4014.

definition of an "operator" when such platforms merely offer the public access to child-directed apps.[127]

3. *The Definition of a "Website or Online Service Directed to Children"*

The amended Rule expands the definition of a "website or online service directed to children" to include third parties, such as plug-ins and advertising networks, that have actual knowledge that they are collecting personal information from a child-directed site or online service.[128] In addition, the definition also includes sites and services that target children only as a secondary audience, so that such sites and services must differentiate among users and comply with the COPPA requirement for users younger than thirteen years old.[129]

4. *"Support for Internal Operations" Exemption from COPPA Coverage*

The amended Rule permits collection and use of children's personal information for internal organizational purposes or uses that "maintain or analyze" the functions of a website or service, or that protect the "security or integrity" of the site or service.[130] Under this definition, functions such as intellectual property protections, payment and delivery, spam protections, optimization, statistical reporting, or de-bugging need not comply with the COPPA requirement.[131] Online behavioral advertising,[132] however, is not included in activities that support internal operations and

[127] *See id.* at 3977. Mobile platforms are, therefore, not required to verify that the apps they sell comply with COPPA. *See id.* at 3977. The individual app developers, on the other hand, must comply with the COPPA requirement. *See id.* at 4009.

[128] *See id.* at 3975.

[129] *See id.*

[130] *Id.*

[131] *See id.*

[132] "Online behavioral advertising" is advertising that specifically targets an individual based on his personal information and web browsing patterns obtained through tracking his web browsing history. *See* Tene & Polonetsky, *supra* note 21, at 282–84.

must comply with COPPA.[133] Moreover, persistent identifiers are not "personal information" where the sole purpose of their collection is to provide support for the operator's internal operations.[134]

5. *Revised Parental Consent Mechanisms*

The original Rule of 1999 recognized a signed parental consent form and a parent's credit card number as appropriate methods to obtain "verifiable parental consent."[135] The amended Rule has added several new methods that operators can use to obtain "verifiable parental consent," including electronic scans of signed parental consent forms, video-conferencing, government-issued identification, and alternative payment systems such as debit cards and electronic payment systems.[136] Further, the amended Rule has retained the sliding-scale mechanism of parental consent, also known as "e-mail plus," as an acceptable consent method for operators that collect personal information only for internal use.[137] Under the "e-mail plus" method, operators may obtain verifiable parental consent with an e-mail from the parent, as long as the operator confirms consent by sending a delayed e-mail confirmation or a letter to the parent or by calling the parent.[138]

6. *Revised Notice Requirement*

The amended Rule has revised the parental notice provisions to ensure that operators provide concise and timely privacy policies and direct notices before collecting children's personal information.[139] The required direct parental notice now specifically

[133] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. at 3979–80.
[134] *See id.* at 3977, 4012 (to be codified at 16 C.F.R. § 312.5(c)(7)).
[135] *See* 16 C.F.R. § 312.5(b)(2) (2012).
[136] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. at 4011.
[137] *See id.* The FTC considered numerous comments on the "e-mail plus" provision. *See id.* at 3999. The FTC concluded that "e-mail plus" remains a valued and cost-effective consent mechanism for certain operators. *See id.* The FTC encourages the development of new efficient and cost-effective consent methods that are more reliable and more verifiable than e-mail plus, such as digital signatures. *See id.* at 3991.
[138] *See id.* at 4011.
[139] *See id.* at 4010.

includes information already collected from the child, the purpose of the notice, the action that the parent must or may take, and what use the operator will make of the personal information collected.[140]

In sum, the amended Rule aims to address expanding needs for children's privacy protection in today's technological landscape by expanding activities and entities subject to COPPA and to close loopholes and clarify the notice and parental consent framework.

IV. PROBLEMS APPLIED TO VIRTUAL EDUCATION

As discussed previously in Part II.B, K–12 schools are increasingly using computer- and Internet-based virtual education. The use of the Internet and mobile apps poses numerous threats and unique challenges related to children's online privacy.[141] Under the current COPPA framework, as addressed by the amended Rule, app developers and website operators targeting K–12 education are now subject to COPPA, just like other commercial app developers and website operators.[142]

The amended Rule should succeed in expanding privacy protection regarding the online activity of young children under the age of thirteen. The amended Rule addresses some of the gaps that

[140] *See id.* In addition to the six provisions described, the amended COPPA Rule: (7) requires operators to take "reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security, and integrity of such information, and who provide assurances that they will maintain the information in such a manner," to retain children's personal information "for only as long as is reasonably necessary," and to protect against unauthorized access while the information is disposed of, *see id.* at 3995, 4012; and (8) strengthens the FTC's oversight of self-regulatory safe harbor programs by requiring the programs to audit their members and to report annually to the FTC the aggregated results of the audits, *see id.* at 3992, 4012. See 15 U.S.C. § 6503 (2006), for the COPPA "safe harbor" provision providing operators with "safe harbors," where an operator may satisfy the COPPA Rule requirements by following self-regulatory guidelines approved under 15 U.S.C. § 6502(b).

[141] *See supra* notes 12–13 and accompanying text.

[142] *See* 15 U.S.C. § 6502; Children's Online Privacy Protection Rule, 78 Fed. Reg. at 4009–11 (providing no exceptions for educational website operators and app developers).

previously existed regarding third-party services and apps. How successful the amended Rule will be in accomplishing its objectives, without causing additional undue burdens, costs, and litigation, is anyone's guess.

Nevertheless, the recently amended Rule still appears not to fully or effectively address online privacy concerns in virtual education. Generally, the FTC revisions have come under some criticism. One commentator complained that the amended Rule's provisions "are riddled with innumerable ambiguities and questionable policy choices"[143] and that the Rule's amendment "is less happy for vendors to kid-oriented websites or apps, including ad networks and app plug-ins, and for kid-oriented websites that haven't already complied with COPPA" where the FTC "wanted to crack down on these COPPA workarounds, but in typical FTC fashion, it did so in a ham-fisted and marble-mouthed way."[144]

For example, one of the amended Rule's definitions is particularly ambiguous and confusing. The Rule applies to any "Web site or online service *directed* to children," which the Rule defines as any "commercial website or online service, or portion thereof, that is *targeted* to children."[145] In the same section, the Rule exempts any website or service "*directed* to children . . . but that does not *target* children as its primary audience" if it meets certain criteria.[146] So, is there a distinction between "directed" and "targeted"? Hard to tell. Such confusion only exacerbates the problems educational and other web providers and app developers face in attempting to comply with COPPA.

In general, the FTC has paid little attention to the impact of COPPA on virtual education, educators, and educational web

[143] Eric Goldman, *The FTC's New Kid Privacy Rules (COPPA) Are a Big Mess*, TECH. & MKTG. L. BLOG (Dec. 27, 2012), http://blog.ericgoldman.org/archives/2012/12/the_ftcs_new_ki.htm.

[144] *Id.*

[145] Children's Online Privacy Protection Rule, 78 Fed. Reg. at 4010 (emphasis added).

[146] *Id.* (emphasis added).

developers.[147] Regrettably, the FTC missed a golden opportunity to squarely address the role of educators and some of the unique challenges of implementing COPPA in virtual education.

Many questions remain regarding the implications of COPPA and the amended Rule's relation to virtual education. Some of the most significant concerns are addressed below.

A. *School Officials' Roles in the Parental Consent Process*

Educational websites and apps are subject to the COPPA regulation, and the COPPA consent provisions must be met before students may use Internet-based learning modules.[148] COPPA and its original Rule, however, were silent regarding school officials' roles in authorizing students to use the Internet at school.[149] When the FTC promulgated the original COPPA Rule in 1999, it stated that the Rule does not preclude public school officials from serving as parental intermediaries or agents in providing verifiable consent.[150] The FTC also created a website titled "How to Protect

[147] *See id.* at 3972–4014 (providing no specific provision or consideration for virtual education in the amended COPPA Rule).

[148] *See supra* text accompanying note 128.

[149] *See* David Hostetler, *School Cyberlaw*, *in* EDUCATION LAW IN NORTH CAROLINA § A.901(G) (Janine Murphy ed., 2004).

[150] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,903 (Nov. 3, 1999) (to be codified at 16 C.F.R. pt. 312). It provided:

> Numerous commenters raised concerns about how the Rule would apply to the use of the Internet in schools. Some commenters expressed concern that requiring parental consent for online information collection would interfere with classroom activities, especially if parental consent were not received for only one or two children. In response, the Commission notes that the Rule does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parents' agent in the process. For example, many schools already seek parental consent for in-school Internet access at the beginning of the school year. Thus, where an operator is authorized by a school to collect personal information from children, after providing notice to the school of the operator's collection, use, and disclosure practices, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent.

Kids' Privacy Online: A Guide for Teachers," which provides that "[s]ubject to [a] school district's policies, [a teacher] may act on behalf of the parent in giving consent, but COPPA does not require [the teacher] to do so."[151]

The specific meaning and significance of FTC guidance has remained unclear since it was first issued following the original Rule's adoption.[152] The FTC does not appear to have ever provided more specific guidance.[153] The amended Rule remains silent regarding school officials' intermediary role.[154]

The Software & Information Industry Association ("SIIA"), in its December 2011 letter to the FTC, encouraged the agency "to take steps to ensure that [the Rule] applied as efficiently as possible with respect to school-based educational partners and other providers of educational materials and services" and to avoid COPPA becoming "an unnecessary barrier to students under age 13 who are seeking access to teaching and learning opportunities important to their formal, academic education . . . ."[155] The SIIA also suggested that the FTC provide more clarity and certainty

---

> Operators may wish to work with schools to educate parents about online educational activities that require websites to collect personal information in the school setting. To ensure effective implementation of the Rule, the Commission also intends to provide guidance to the educational community regarding the Rule's privacy protections.

Id. (footnote omitted).

[151] *FTC—How to Protect Kids' Privacy Online: A Guide for Teachers*, BBB NEWS CTR. (Dec. 1, 2002), http://www.bbb.org/us/article/ftc--how-to-protect-kids-privacy-online-a-guide-for-teachers-4550.

[152] *See* Hostetler, *supra* note 149 (Co-author David Hostetler noting these concerns).

[153] *See id.*

[154] *See* Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 3972–4014 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312) (providing no specific provision or consideration for virtual education in the amended COPPA Rule).

[155] Letter from Ken Wasch, President, Software & Info. Indus. Ass'n, to Donald S. Clark, Secretary, Fed. Trade Comm'n 14 (Dec. 23, 2011), *available at* http://www.ftc.gov/os/comments/copparulereview2011/00363-82389.pdf.

about its regulations, rather than rely on less formal and dependable agency guidance.[156]

An amendment to COPPA, regulatory modification, or more specific agency guidance that would allow school officials to serve as "parental representatives," rather than just "intermediaries" for parental consent, would strike a better balance between protecting privacy and encouraging time-efficient and minimally burdensome requirements on already overburdened school officials.

B. *No Educational Exception or Safe Harbor Regarding Parental Consent*

Perhaps the most direct way to foster efficiency in virtual education efforts is to eliminate the need for direct parental consent when schools and school officials facilitate virtual education. Interestingly, when it adopted the original Rule, the FTC considered and rejected a proposal that the Rule allow exceptions for parental consent in instances when schools collaborate with web providers for online educational purposes, stating that the FTC did not have discretion under the statute to waive the requirement of verifiable parental consent.[157]

The public puts its trust in school officials in many ways to protect its underage students in other contexts relating to other safety threats. People commonly expect school officials to act on parents' behalf to protect students against bullying, harassment, illegal drug and alcohol use, and other kinds of threats.[158] Schools,

---

[156] *Id.* at 15 ("SIIA urges the commission to codify this distinction in the regulation to ensure all stakeholders have certainty about these regulations, rather than relying on less formal and less dependable FAQ guidance.").

[157] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,909 (Nov. 3, 1999) (to be codified at 16 C.F.R. pt. 312) ("According to [one] commenter, a child's use of collaborative educational tools on the Internet should be treated differently from the collection and use of personal contact information by marketers. The commenter, who called for parental notification and opt-out for such collaborative uses, was especially concerned about the loss of business from schools. The Commission does not have discretion under the statute to waive the requirement of verifiable parental consent.").

[158] Title IV of the Civil Rights Act of 1964 and Title IX of the Educational Amendments of 1972 impose duties on schools receiving federal funding to

then, should be able to act on parents' behalf in the best interests of students to guard student privacy in the context of online schooling, as well. Consequently, it seems reasonable, particularly in light of expanding online education and limited school resources, to authorize school officials to review privacy policies of online educational operators and to provide consent in lieu of parents for children's use of online educational materials at school, while reserving parents' rights to opt-out.[159] It would be prudent to amend COPPA itself, if the FTC believes its hands are tied.

For the present, without a codified educational exception, educators and educational web providers subject to COPPA must find efficient ways to develop and offer online educational opportunities while simultaneously complying with COPPA. One practical solution is for the online education community to develop effective and easily manageable safe harbor guidelines approved

---

prohibit discrimination and harassment against students based on race and gender, respectively. *See* Civil Rights Act of 1964, Pub. L. No. 88-352, tit. IV, 98 stat. 241, 246 (1964) (codified at 42 U.S.C. §§ 2000c–2000c-9 (2006)); Educational Amendments of 1972, Pub. L. No. 92-318, tit. IX, 86 stat. 235, 373–75 (June 23, 1927) (codified at 20 U.S.C. §§ 1681–1688 (2006)). For additional examples of expectation of the public that schools would protect children on parents' behalf see Bd. of Educ. v. Earls, 536 U.S. 822, 830 (2002) (recognizing responsibility of the state in "maintaining discipline, health, and safety" of school children); Morse v. Frederick, 551 U.S. 393, 408 (2007) ("Student speech celebrating illegal drug use at a school event, in the presence of school administrators and teachers, thus poses a particular challenge for school officials working to protect those entrusted to their care from the dangers of drug abuse."); KERN ALEXANDER & M. DAVID ALEXANDER, AMERICAN PUBLIC SCHOOL LAW 509 (8th ed. 2011) ("The safety of students is always a compelling consideration of the school and the courts place safety in a high-priority position when viewing any action by a school district.").

[159] Many schools, particularly public schools, usually have grievance or other textbook procedures available to parents to determine whether to allow a student to "opt out" of a particular assignment that a parent finds objectionable. *See Parental Rights in Education*, ACLJ, http://aclj.org/education /parental-rights-in-education (last visited Mar. 2, 2013). This is not the same as requiring affirmative consent for each assignment. Similarly, schools could and often do offer an "opt out" for school internet use. *See id.*

by the FTC as allowed by COPPA.[160] Having such safe harbors provides companies subject to COPPA with clear guidelines and expectations, reducing legal uncertainties and costs. For example, TRUSTe is a web-based privacy protection service whose licensees comply with specific privacy protocols established by TRUSTe and which are COPPA-compliant and approved as "safe harbor practices" by the FTC.[161] TRUSTe licensees have contractually bound themselves to the TRUSTe protocols.[162] When licensees post the TRUSTe seal on their website, users have reasonable assurance that the particular website provider follows effective privacy protection practices.[163]

---

[160] *See* 15 U.S.C. § 6503 (2006); Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 4012–13 (Jan. 17, 2013) (to be codified at 16 C.F.R. § 312.11).

[161] *About TRUSTe*, TRUSTE, http://www.truste.com/about-TRUSTe/ (last visited Mar. 17, 2013).

[162] TRUSTe Children's License Agreement, FED. TRADE COMM'N, *available at* http://www.ftc.gov/privacy/safeharbor/trustelicenseagreement.pdf (last visited May 22, 2013). According to the TRUSTe license agreement:

> Licensees with online activities that are directed at children under the age of 13, or that have actual knowledge that they are collecting or maintaining personal information from children under the age of 13, must display TRUSTe's Children's Mark and must abide by Schedule A, Children's Program Requirements . . . .
>
> TRUSTe's Children's Program Requirements will be modified as necessary to meet the requirements of the Children's Online Privacy Protection Act (COPPA) and its implementing Rule, 16 C.F.R. Part 312. TRUSTe's Children's Program has been approved by the Federal Trade Commission as an authorized safe harbor under the COPPA rule. All Licensees are required to meet the requirements of the Children's Program and the COPPA rule.

Id.

[163] *See Children's Privacy Seal*, TRUSTE, http://www.truste.com/products-and-services/enterprise-privacy/coppa (last visited Mar. 17, 2013) ("The Federal Trade Commission has approved TRUSTe as a COPPA Safe Harbor program. The TRUSTe Children's Seal certifies that your business is compliant with the COPPA Rule—letting parents know that their kids' information is safe.").

C. *Educator Responsibility, Risk, and Liability Concerns*

It is unclear who is legally responsible, and how, if parents are not properly afforded their COPPA rights in cases of virtual education administered or mediated by school officials. Some educational web providers attempt to deflect parental consent responsibility by informing school officials that it is their responsibility to obtain parental consent in order to use the provider's services.[164] In some cases, this is part of a licensing agreement.[165] Examples include Gaggle,[166] McGraw-Hill online testing service,[167] and Edmodo.[168]

---

[164] *See infra* notes 166–68.

[165] *See infra* notes 166–68.

[166] *See Gaggle's Privacy Statement*, GAGGLE 3, *available at* http://shadowridge.adams12.org/gaggle/Gaggle%20Privacy%20Statement.pdf ("Use of the Free Version of Gaggle implies that your school is acting as a proxy for parental consent and agrees to the advertising, data collection, and terms of service of the Gaggle web site.").

[167] *See COPPA Policies*, MCGRAW HILL LLC, https://oas.ctb.com/SessionWeb/resources/html/coppa_policy.html (last visited Mar. 17, 2013) ("The administrator of this test is advised that his or her education agency is solely responsible for compliance with the Children's Online Privacy Protection Act of 1998 ('COPPA') as well as other laws applicable to the collection, use and disclosure of personal information about students who will be accessing these services. Administrators should confirm with their agency that they are acting in compliance with all applicable laws relating to the collection, use and disclosure of personal information about students. . . . [A]ny compliance required under COPPA will be the responsibility of the school authority.").

[168] *See Edmodo*, TECH. RESOURCE TCHRS., http://education.fcps.org/trt/edmodo (last visited Mar. 17, 2013) ("If you are accessing the Services on behalf of a school or district, the following terms also apply to you: . . . You represent and warrant that you are solely responsible for complying with the Child Online Privacy Protection Act ('COPPA') . . . . You must obtain advance written consent ('Consent') from all parents whose children will be accessing the Services. You are responsible for understanding how any Third Party Software that you install on behalf of yourself or other users may collect and use information of users of the Edmodo's Services, and you must also obtain Consent from all parents whose children will be using any such Third Party Software that you install. When obtaining Consent, you must provide parents with a copy of our Privacy Policy (located at http://www.edmodo.com/

Thus far, there are no reported cases of lawsuits involving companies who have passed parental consent responsibility to school officials; this vacuum leaves us to speculate about future liability in such instances. The uncertainties leave stakeholders to worry about and struggle to find ways not to be the "test case" in such instances. Without regulatory clarification, it appears that schools relying on such online educational services are expected to accede to the COPPA parental consent terms imposed by online providers. School attorneys and officials will have to carefully weigh the implications when deciding if the online opportunities are worth the risks.

D. *The Amended Rule's Inhibiting Effect on Online Educational Innovation and Opportunities*

Commonly expressed concerns about the amended Rule, with its expanded coverage to app developers and third-party vendors, include the potential chilling impact it will have on the development of useful child-oriented and educational apps as well as the Rule's potential violation of the First Amendment.[169]

It remains to be seen, though difficult to measure, how inhibiting the amended Rule will actually be on innovation in virtual education, particularly on educational apps and other newly

---

corporate/privacy-policy). You must keep signed Consents on file and provide them to Edmodo upon our request. For more information on COPPA, please see www.ftc.gov/privacy.").

[169] *See, e.g.*, Sasha Grandison, Comment, *The Child Online Privacy Protection Act: The Relationship Between Constitutional Rights and the Protection of Children*, 14 UDC/DCSL L. REV. 209, 219–20 (2011) (illustrating criticisms that the COPPA framework places an undue burden on commercial website operators, resulting in disallowance of children's access to its website or shutdown of its website, as well as that COPPA infringes the First Amendment rights of websites by forcing them to self-censor their content); Gabe Rottman, *FTC Proposes Changes to Privacy Law that Collide With free Speech*, AM. CIV. LIBERTIES UNION (Sept. 26, 2012, 11:59 AM), http://www.aclu.org/blog/technology-and-liberty-human-rights-free-speech/ftc-proposes-changes-privacy-law-collide-free (expressing concerns that general purpose sites will become more mature to avoid attracting children, raising fears that government would be influencing the content of online speech protected by the First Amendment).

encompassed web providers and services. In response to the amended COPPA Rule, the executive director representing an app developer community of "tens of thousands of independent app developers" commented that many of these developers were individuals or very small companies with very limited resources and would face the dilemma of whether to produce educational apps when faced with the prospects of expensive legal fees to comply with COPPA or just to determine that a developer was not subject to COPPA.[170]

V. RECOMMENDATIONS: COPPA AND VIRTUAL EDUCATION

The prior discussion addresses how COPPA and the amended Rule affect virtual education, as well as what educators can and must do within the existing COPPA framework.[171] This Part elaborates on recommendations for future modifications and

[170] In response to the amended COPPA Rule, Association for Competitive Technology Executive Director Morgan Reed stated:

> Today, tens of thousands of independent app developers from around the country are building the future of education. . . .
>
> These innovators want to provide groundbreaking educational innovations while protecting the privacy of their users, but $9,500 in legal fees represents more than a year's worth of income for most educational apps. Moreover, even if an app does not actually require COPPA parental consent, the complexity of these rules will require most educational app developers to spend thousands of dollars in legal fees to confirm one way or another.
>
> We are very concerned about the implementation of this rule, especially as it applies to the use of third party plug-in technologies that make the app ecosystem possible. . . . [Some are] suggesting the eventual implementation of the new [COPPA] rules would make it difficult for educational app startups to survive. While large, vertically-integrated firms like Google never need to use third party plug-ins, the startup community is dependent on analytics, classroom tools, and other services provided by their partners.

COPPA—Improved for Big Companies, Not for Education Startups, ASS'N FOR COMPETITIVE TECH., http://actonline.org/pressreleases/2012/12/19/coppa-%E2%80%93-improved-for-big-companies-not-for-education-startups/ (last visited Mar. 17, 2013).

[171] *See supra* Part IV.

clarifications of COPPA and the Rule to improve COPPA's application to virtual education.

A. *Parental Consent Exception-Presumption*

The time seems ripe, with the rapid increase in online education, for the Rule or the Act itself to make an exception for, or to presume, parental consent for legitimate school-sponsored virtual education facilitated by authorized school officials (the "consent exception-presumption").[172] The SIIA, representing website operators, urged such an exception before the amended Rule was adopted.[173] Specifically, it called for amending Section 1303(b)(2)(c)(ii) of the COPPA statute to provide the FTC with authority to craft exceptions to the parental consent requirement "taking into consideration the benefits to the child of access to information and services" as an effective way to maximize educational opportunities and still protect children's privacy.[174] Alternatively, such an amendment could be tailored to be a presumption of consent, rather than an outright exception to it.

The policy rationale for this parental exception-presumption is based on the notion that school officials already act on behalf of students' educational best interests and wellbeing when arranging and delivering their education in non-virtual contexts.[175] School officials and educators have assumed, and must continue to assume, such roles in their decisions and supervision: for example, the suitability of curricula and texts; school safety and emergency practices; student discipline; administering medicines and first-aid; organizing and supervising athletics, chemistry labs, shop classes, and other high-risk activities.[176] For much of America's educational

[172] "Legitimacy" should involve a common-sense notion of any school that is publicly recognized as an established school: e.g., state-supported public schools or accredited private schools. The authors do not attempt, here, to define the term more specifically.

[173] *See* Wasch, *supra* note 155, at 15.

[174] *Id.*

[175] *See, e.g.*, ALEXANDER & ALEXANDER, *supra* note 158, at 636 (stating that school discipline should meet a standard that includes consideration of a student's, as well as the school's, best interests).

[176] *See id.*

history, education officials and courts have acknowledged, to varying degrees, the notion that educators act *in loco parentis*—"in place of a parent" in such instances.[177] At the least, it is commonly recognized that educators assume a supervisory role in which they are responsible for providing reasonable care and instruction to students.[178]

There may be nothing quantitatively or qualitatively unique about children's online educational practices and privacy risks for which educators are not sufficiently suited to make proper decisions—in place of parents—when facilitating virtual education. To require one more administrative step—obtaining individual parental consent—saddles already overburdened educators and schools with one more level of effort and is likely to further hinder the delivery of effective online education.

In response to any concern that parents should retain the ultimate right to withhold consent for online learning, the law could include a parental educational opt-out provision if the law was amended to include just a presumption of parental consent (rather than a complete exception to it). This would be consistent with other recognized school practices. It is well known, for example, that schools typically allow parents to request to opt out of having their children use specific curricular materials, like those

[177] *See, e.g.*, Morse v. Frederick, 551 U.S. 393, 416 n.6 (2007) (Thomas, J., concurring) ("At least nominally, this Court has continued to recognize the applicability of the *in loco parentis* doctrine to public schools."); *see also* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654–55 (1995) ("Traditionally at common law, and still today, unemancipated minors lack some of the most fundamental rights of self-determination . . . . They are subject . . . to the control of their parents or guardians. When parents place minor children in private schools for their education, the teachers and administrators of those schools stand *in loco parentis* over the children entrusted to them." (internal citations omitted)); Bethel Sch. Dist. No. 403 v. Fraser, 478 U.S. 675, 684 (1986) ("These cases recognize the obvious concern on the part of parents, and school authorities acting *in loco parentis*, to protect children—especially in a captive audience—from exposure to sexually explicit, indecent, or lewd speech."); ALEXANDER & ALEXANDER, *supra* note 158, at 634 ("The courts still uphold the ancient doctrine of *in loco parentis*, which holds that the teacher stands in place of the parent and in such capacity has the right to chastise a pupil.").

[178] *See* ALEXANDER & ALEXANDER, *supra* note 158, at 509.

containing certain mature content or sex-education materials, or from engaging in special school activities, such as field trips or saying the pledge of allegiance.[179]

B. *Educational Safe Harbors*

In addition to a parental consent exception or presumption, the law should also encourage virtual education innovation and opportunities by providing safe harbor provisions for online education website operators and app developers.[180] To do so, the law should define "online" or "virtual education" entities and the scope of applicability of online education safe harbor provisions. Generally, the following guidelines are suggested as a baseline for qualifying for a safe harbor: (1) the provider's objectives and services are primarily for educational purposes and aimed at students and schools for online education;[181] (2) the personal information obtained from users will be used only for educational purposes; and (3) the personal information shall not be retained any longer than necessary to fulfill the provider's educational purposes and users' needs.[182]

C. *Clarify Educators' Roles as Parental Intermediaries*

Modification of COPPA or the Rule to codify or clarify the role of school officials as parental intermediaries would be extremely helpful.[183] The authors agree with the recommendations and reasoning of SIIA on this matter.[184] Having been relatively

---

[179] *See Parental Rights in Education*, *supra* note 159.

[180] Having online educational safe harbors would provide companies subject to COPPA with clear guidelines and expectations, reducing legal uncertainties and costs. *See supra* Part IV.B.

[181] "Online" or "virtual education" should also be defined in this context.

[182] Short of explicit educational safe harbors added directly to COPPA or the Rule, the online education community can at least develop its own safe harbor guidelines and have them approved by the FTCs previously mentioned COPPA safe harbor allowances. *See* 15 U.S.C. § 6503 (2006); Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 4012–13 (Jan. 17, 2013) (to be codified at 16 C.F.R. § 312.11).

[183] *See supra* Part IV.A.

[184] *See supra* note 156 and accompanying text.

silent in this regard for almost fifteen years, the time has come for the FTC to speak up. The government can spare schools and providers much uncertainty and costs if the FTC prescribes a set of procedures, or even just offers a recommended parental consent form or method and a set of specific guidelines for virtual education purposes.

D. *Clarify the Responsibility of Educators*

It remains unclear how liability of schools and educational providers covered by COPPA might apply where parental COPPA rights are violated involving virtual education.[185] As noted above, there is a practice of some educational providers covered by COPPA to pass responsibility for parental consent to educational users of such providers' services.[186] The law should be amended to address this practice and clarify the extent to which covered providers may require educators to assume such responsibility and, if they fail to do so in violation of COPPA, how the law applies.

E. *Other Options and Considerations*

There are other ways to improve legislation for the sake of protecting children's privacy in the context of virtual education. For example, due to the dangers faced by students older than twelve, there should be continuing consideration as to whether the COPPA framework should be expanded, perhaps in more limited ways, to protect older students.[187] Dangers of such expansion might potentially infringe on older minors' First Amendment rights, as well as pose an undue obstruction to educational innovation and services.[188] The question should remain on the table and research conducted to determine if protecting students, as old

[185] *See supra* Part IV.C.

[186] *See supra* Part IV.C.

[187] *See, e.g.*, Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. 13 (2011) (proposing amendments to COPPA to, among other things, extend to all children under the age of eighteen). This bill was not enacted. *See H.R. 1895 (112th): Do Not Track Kids Act of 2011*, GOVTRACK.US, http://www.govtrack.us/congress/bills/112/hr1895 (last visited May 22, 2013).

[188] *See supra* note 169 and accompanying text.

as eighteen, will be necessary as their online educational use continues to expand.

Another example is a potential legislative restriction of online tracking of user information. The Do-Not-Track Online Act of 2013, Senate Bill 418,[189] aims to require a mechanism by which an individual can opt out of collection of personal information by online service operators including mobile app developers and to prohibit operators from collecting personal information from opted-out individuals.[190] While the underlying notion of protecting online privacy is a great one, the broad scope of the Bill may deprive users of means for Internet customization and interfere with the Internet content.[191] At the same time, the Bill may be ineffectively enforced, leaving many loopholes including regulation of social networking websites where Internet advertising increasingly takes place.[192]

In sum, regulatory efforts to enhance children's online privacy must carefully balance the protection of children's privacy with efficient access to useful and educational Internet resources.

VI. CONCLUSION

This article has reviewed the background and requirements of COPPA and the amended Rule, noted areas of concern, and suggested improvements and necessary practices in the context of virtual education. Undoubtedly, over time two things are likely to expand further: the availability and use of the Internet for life's purposes, including online education, and corresponding threats to users' and children's privacy and safety. The COPPA regulatory framework is a significant effort to protect the privacy of our

[189] Do-Not-Track Online Act of 2013, S. 418, 113th Cong. (2013).

[190] *See id.* § 2. The Do-Not-Track Online Act of 2013 is a re-introduction of the Do-Not-Track Online Act of 2011. *See* S. 913, 112th Cong. (2011). A similar House Bill was also previously introduced. *See* Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011).

[191] *See* Stephanie A. Kuhlmann, Legislative Update, *Do Not Track Me Online: The Logistical Struggles over the Right "to be Let Alone" Online*, 22 DEPAUL J. ART TECH. & INTELL. PROP. L. 229, 284 (2011).

[192] *See id.*

nation's youth. It can become easily outdated, however, in the context of rapidly developing Internet technology. The FTC should, among other things, clarify educator roles and responsibilities in the COPPA process and address educational providers' efforts to shift parental consent responsibility to educators.

Finally, all stakeholders—regulators, educators, educational providers, parents, and children—will need to consider and improve on efforts regarding the disclosure of information, understanding of COPPA requirements, facilitation of consent, and, most importantly, ways to protect our nation's children while taking advantage of increased online education. Educators and online educational providers must collaborate and, together, educate students and parents on safe and effective online learning practices. Parents and educators must increase their awareness of, and proficiency in, navigating and taking advantage of the Internet for online educational purposes. With these efforts, students can be both safer and better educated.

14 N.C. J.L. & TECH. ON. 167, 204
Protecting Children's Privacy in Virtual Education