THE PROGRESS & FREEDOM FOUNDATION

Progress on Point

Volume 16, Issue 11 June 2009

COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech

by Berin Szoka & Adam Thierer*

Executive Summary

Online privacy, child safety, free speech and anonymity are on a collision course. The 1998 Children's Online Privacy Protection Act (COPPA) already mandates certain online privacy protections for children under 13, but many advocate expanding online privacy protections for both adolescents and adults. Furthermore, efforts continue at both the federal and state levels to institute new regulations, such as age verification mandates, aimed at ensuring the safety of children online. There is an inherent tension between these objectives: Attempts to achieve perfectly "safe" online environments will likely require the surrender of some privacy and speech rights, including the right to speak anonymously.

These tensions are coming to a head with state-based efforts to expand COPPA, which requires "verifiable parental consent" before certain sites or services may collect, or enable the sharing of, personal information from children under the age of 13. Several proposed state laws would extend COPPA's parental-consent framework to cover all adolescents under 18. This seemingly small change would require age verification of not only adolescents and their parents, but—for the first time—large numbers of adults, thus raising grave First Amendment concerns. Such broad age verification mandates would, ironically, *reduce* online privacy by requiring *more* information to be collected from both adolescents and adults for age verification purposes, while doing little to make adolescents safer. In practical terms, the increased scale of "COPPA 2.0" efforts would present significant implementation and enforcement challenges. Finally, state-level COPPA 2.0 proposals would likely conflict with the Constitution's Commerce Clause.

Despite these profound problems, COPPA expansion has great rhetorical appeal and seems likely to be at the heart of future child safety debates—especially efforts to require mandatory age verification. There are, however, many better ways to protect children online than by expanding COPPA beyond its original, limited purpose.

---

* Berin Szoka (bszoka@pff.org) is a Fellow with The Progress & Freedom Foundation (PFF) and the Director of PFF's Center for Internet Freedom. Adam Thierer (athierer@pff.org) is a Senior Fellow with PFF and the Director of PFF's Center for Digital Media Freedom. The views expressed here are their own, and are not necessarily the views of the PFF board, other fellows or staff. The authors wish to thank Jim Dunstan, Anne Collier, and Braden Cox for their constructive suggestions.

Table of Contents

I. Introduction

When the debate about social networking safety first heated up a few years ago, some state attorneys general (AGs) and vendors of age verification services implied that the technology existed—or could be easily developed—to verify the age of any minor who sought access to an interactive website.[1] Federal law currently requires—via the Children's Online Privacy Protection Act (COPPA) of 1998[2]—that child-oriented website operators or service providers "Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children [under 13]."[3] But advocates of age verification mandates have argued that online child safety would be improved if websites—particularly "social networking

1. *See, e.g.,* Emily Steel & Julia Angwin, *MySpace Receives More Pressure to Limit Children's Access to Site*, Wall Street Journal, June 23, 2006, http://online.wsj.com/public/article/SB115102268445288250-YRxkt0rTsyyf1QiQf2EPBYSf7iU_20070624.html.

2. 15 U.S.C. § 6501–6506.

3. *See* 16 C.F.R. § 312.5. *See infra* at 6 and note 25 for a discussion of COPPA's other requirements, particularly that COPPA applies if a website has "actual knowledge" that it is collecting information from a child even if the website is not "directed at" children.

sites" like MySpace, Facebook and Bebo—were required to do more: screen users by age and to limit or ban access by those over, or under, a certain age.

Today, however, the practical limitations and dangers of age verification mandates have become more widely recognized. Few continue to argue for directly mandating verification of the age of minors online—or that such verification, in its strictest sense, is even technically feasible. Federal courts have found that there is "no evidence of age verification services or products available on the market to owners of Web sites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor."[4] Few public databases exist that could be referenced to conduct such verifications for minors, and most parents do not want the few records that *do* exist about their children (*e.g.*, birth certificates, Social Security numbers, school records) to become more easily accessible.[5] Indeed, concerns about those records being compromised or falling into the wrong hands have led to legal restrictions on their accessibility.[6]

There are a host of other concerns about age verification mandates.[7] Some of these concerns were summarized in a recent report produced by the Internet Safety Technical Task Force, a blue ribbon task force assembled in 2008 by state AGs to study this issue:

> Age verification and identity authentication technologies are appealing in concept but *challenged in terms of effectiveness*. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues.[8]

---

4. ACLU v. Gonzales, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007) [hereinafter *Gonzales*]; *see infra* at 28.

5. *See* Adam Thierer, The Progress & Freedom Foundation, *Age Verification Debate Continues; Schools Now at Center of Discussion*, PFF Blog, Sept. 25, 2008, http://blog.pff.org/archives/2008/09/age_verificatio_1.html.

6. Various laws and regulations have been implemented that shield such records from public use, including various state statutes and the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

7. For a fuller exploration of these issues, *see* Adam Thierer, The Progress & Freedom Foundation, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, Progress on Point No. 14.5, Mar. 2007; Adam Thierer, The Progress & Freedom Foundation, *Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General*, Jan. 14, 2008, www.pff.org/issues-pubs/other/090114ISTTFthiererclosingstatement.pdf; Nancy Willard, *Why Age and Identity Verification Will Not Work—And is a Really Bad Idea*, Jan. 26, 2009, www.csriu.org/PDFs/digitalidnot.pdf; Jeff Schmidt, *Online Child Safety: A Security Professional's Take*, The Guardian, Spring 2007, www.jschmidt.org/AgeVerification/Gardian_JSchmidt.pdf.

8. Internet Safety Technical Task Force, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys*

With opposition to strict age verification mandates growing, some regulatory advocates now seek to institute such mandates through the back door of "parental consent" mandates in the model of COPPA. Such "COPPA 2.0" legislation has been introduced at the state level that would extend the COPPA parental-consent framework to cover all minors between the ages of 13 and 17 inclusive ("adolescents"). Some of these bills would also broaden the range of sites covered, increase the amount of information required to be collected to achieve "verifiable parental consent" or impose other mandates such as parental access.

Two such bills were introduced in 2007, in North Carolina (with the support of that state's Attorney General Roy Cooper)[9] and Georgia.[10] While these bills were never passed, a similar bill is currently pending in Illinois.[11] Because the scope of such bills would reach *all* "social networking sites" that offered certain functionality (*e.g.*, user profiles), rather only those sites directed at a particular age bracket (as under COPPA),[12] they would extend age verification mandates far beyond sites that might be considered "adolescent-oriented." Another bill is currently pending in New Jersey; like COPPA, this bill would reach only sites directed at adolescents, but it might reach a broader range of sites, because its scope is not limited specifically to "social networking" functionality.[13] The introduction of these bills makes it clear that future online identity verification debates will be increasingly tied up with efforts to expand the COPPA framework. These mandates will likely arrive in the form of state-level expansions of, or federal amendments to, COPPA, or such proposals will at least cite COPPA's regulatory framework as precedent. Yet COPPA 2.0 advocates seem to forget that, back in 1998, Congress considered, but ultimately rejected, a requirement in the original version of COPPA that operators make "reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17."[14] This requirement would have been significantly less burdensome than the COPPA 2.0 approaches advanced today, but it was

---

General of the United States, Dec. 31, 2008, at 10, http://cyber.law.harvard.edu/pubrelease/isttf [hereinafter *ISTTF Final Report*]. Full disclosure: Adam Thierer was a member of this task force.

9. S.B. 132, 2007 Gen. Assem., Reg. Sess. § 8 (N.C. 2007), *available at* www.ncga.state.nc.us/Sessions/2007/Bills/Senate/HTML/S132v3.html; *see also* Roy Cooper, *Protecting Children from Sexual Predators: SB 132*, July 24, 2007, www.ncdoj.com/DocumentStreamerClient?directory=WhatsNew/&file=S132%20Summary%20final.pdf; *see also* Adam Thierer, The Progress & Freedom Foundation, *Age Verification Showdown in North Carolina*, PFF Blog, July 26, 2007, http://blog.pff.org/archives/2007/07/age_verificatio.html.

10. S.B. 59, Gen. Assem., 2007-2008 Leg. Sess. (Ga. 2007), *available at* www.legis.ga.gov/legis/2007_08/fulltext/sb59.htm.

11. H.B. 1312, 96th Gen. Assem., Synopsis as Introduced (Il. 2007) [hereinafter *SNWARA*], *available at* www.ilga.gov/legislation/billstatus.asp?DocNum=1312&GAID=10&GA=96&DocTypeID=HB&LegID=43038&SessionID=76.

12. *See infra* note 22 and associated text (noting that that COPPA also applies in cases of "actual knowledge," even if a site is not "directed at" children); *see also infra* Section V.A (discussing the meaning of "directed at").

13. A.B. 108, Gen. Assem., 213th Leg. Sess. (N.J. 2008) [hereinafter *AOPPA*], *available at* www.njleg.state.nj.us/2008/Bills/A0500/108_I1.HTM.

14. Children's Online Privacy Protection Act, S. 2326, 105th Cong. § 3(a)(2)(iii) (1998).

stricken from the final version of COPPA after likely constitutional and practical problems were identified.[15]

Today's COPPA 2.0 bills are fraught with even greater legal, technical, and other practical problems in that they would:

- Burden the free speech rights of adults by imposing age verification mandates on many sites used by adults, thus restricting anonymous speech and essentially converging—in terms of practical consequences—with the unconstitutional Children's Online Protection Act (COPA),[16] another 1998 law sometimes confused with COPPA;
- Burden the free speech rights of adolescents to speak freely on—or gather information from—legal and socially beneficial websites;
- Hamper routine and socially beneficial communication between adolescents and adults;
- Reduce, rather than enhance, the privacy of adolescents, parents and other adults because of the massive volume of personal information that would have to be collected about users for authentication purposes (likely including credit card data);
- Would likely be the subject of massive fraud or evasion since it is not always possible to definitively verify the parent-child relationship, or because the system could be "gamed" in other ways by determined adolescents;
- Do nothing to prevent offshore sites and services from operating outside these rules;
- Present major practical challenges for law enforcement officials in the face of such evasion by both domestic users and offshore sites;
- Could destroy opportunities for new or smaller website operators to break into the market and offer competing services and innovations, thus contributing to consolidation of online content and services by erecting barriers to entry; and
- Violate the Commerce Clause of the U.S. Constitution, since Internet activity clearly represents interstate commerce that states have no authority to regulate.

There are better approaches to protect adolescents that do not implicate the serious legal and societal issues raised by COPPA 2.0 efforts.[17] Attempts to expand COPPA to cover adolescents are thus unnecessary and misguided and should be rejected at both the state and federal levels.

---

15. Testimony of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology, before the Senate Committee on Commerce, Science and Transportation Subcommittee on Communications, Sept. 23, 1998, *available at* www.cdt.org/testimony/980923mulligan.shtml [hereinafter *Mulligan Testimony*].

16. 47 U.S.C. § 231. While COPPA governs sites "directed at" children, COPA would have required age verification for content deemed "harmful to minors." COPA has been struck down on First Amendment grounds. *See infra* at Section VI.

17. *See generally* Adam Thierer, The Progress & Freedom Foundation, *Parental Controls and Online Child Protection: A Survey of Tools and Methods*, Special Report, Version 3.1, Fall 2008, www.pff.org/parentalcontrols/index.html (cataloguing the tools and methods available to parents to control their kids' Internet use).

The FTC should consider carefully the limitations of COPPA and the pitfalls of COPPA 2.0 as the agency prepares to begin an expedited review of COPPA (five years ahead of schedule).[18]

Before examining in greater detail the problems posed by COPPA 2.0 proposals (Sections IV-VIII), we review how COPPA 1.0 currently works (Section II) and what it achieves (Section III).

Terminology

"**Adult**" – Anyone 18 and over

"**Minor**" – Anyone under 18

"**Child**" – Anyone under 13

"**Adolescent**" – Anyone 13 or over but less than 18

"**Kid**" – Because of the specific meaning of "child" under COPPA, we have used "kid" instead of "child" when discussing interaction with parents and as a colloquial catch-all where appropriate.

"**PI-collecting site**" – Any site that collects what COPPA considers "personal information," which includes contact information.

"**Social networking site**" – A generic term for a PI-collecting site focused on user profiles and connections among users. Some legislative proposals use this term to refer to sites with specific functionality.

II. Current Implementation of COPPA

COPPA generally requires that commercial operators of websites and services obtain "verifiable parental consent" before collecting, disclosing or using "personal information" (*e.g.*, name, contact information)[19] about children under 13[20] if either (i) their website or service (or "portion thereof") is "directed at children"[21] or (ii) they have actual knowledge that they are collecting personal information from a child.[22] Even if sites and services that collect personal information ("PI-collecting sites"[23]) are not "directed at" children, they must

18. Howard Buskirk & Yu-Ting Wang, *FTC to Expedite Review of Children's Online Privacy Protection Rule*, Communications Daily, April 23, 2009, at 5-7.

19. The FTC has defined "personal information" to include:

> (a) A first and last name; (b) A home or other physical address including street name and name of a city or town; (c) An e-mail address or other online contact information, including but not limited to an instant messaging user Identifier, or a screen name that reveals an individual's e-mail address; (d) A telephone number; (e) A Social Security number; (f) A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or (g) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described.

16 C.F.R. § 312.2.

20. The word "child" is sometimes used interchangeably with the legal term "minor" (someone under 18) in federal law. *See, e.g.*, 18 U.S.C. § 2256(1) (defining "minor" as "any person under the age of eighteen years") and 18 U.S.C. § 2256(8) (defining "child pornography" as "any visual depiction… of sexually explicit conduct [involving a minor]"). In common speech, the term "child" is often used to mean "a son or daughter of any age." Dictionary.com, "child," Merriam-Webster's Dictionary of Law, dictionary.reference.com/browse/child. By contrast, COPPA defines "child" as a subset of "minor." COPPA 2.0 bills would apply to older minors not currently subject to COPPA, generally referred to as "adolescents."

21. 16 C.F.R. § 312.2 (definition of "Website or online service directed to children"); *see infra* at 22-24 (discussing the FTC's criteria for deciding what constitutes a site "directed to" children).

22. *See* 16 C.F.R. § 312.3; *see also* 16 C.F.R. § 312.2 (definition of "Website or online service directed to children").

23. We use the term "PI-collecting sites" to refer to both sites and services only for lack of a clearer catch-all.

still have such a process in place to deal with cases in which a child has disclosed that they are under 13. The FTC has defined COPPA's scope so broadly that it could apply even to virtual worlds and multiplayer online games (*e.g.*, Second Life, World of Warcraft).[24] COPPA also requires certain notices about information collection, parental access to information collected about children, reasonable data security procedures, and restrictions on the collection of personal information through games and prizes.[25]

A. The Difficulties in Obtaining "Verifiable Parental Consent"

In drafting the regulations that implemented COPPA (the "COPPA Rule"),[26] the Federal Trade Commission (FTC) in 1999 adopted a "sliding scale" approach to obtaining parental consent.[27] This approach allows operators of PI-collecting sites to use a mix of methods to comply with the law, including print-and-fax forms, follow-up phone calls and e-mails, credit card authorizations and using encryption certificates.[28] The FTC has also authorized four "safe harbor" programs operated by private companies that help website operators comply with COPPA.[29]

---

24. As the FTC has explained:

> COPPA applies to personal information collected online by websites and online services located on the Internet. The Rule defines "Internet" to mean the myriad of computer and telecommunications facilities that make up the world-wide networks that employ the Transmission Control Protocol/Internet Protocol (TCP/IP), or any predecessor or successor protocols used to communicate information of all kinds by wire, radio, or other methods of transmission. See 16 C.F.R. § 312.2 (definition of "Internet"). The Rule's Statement of Basis and Purpose makes clear that the term Internet is intended to apply to broadband networks, as well as to intranets maintained by online services that either are accessible via the Internet, or that have gateways to the Internet.

Federal Trade Commission, *Frequently Asked Questions about the Children's Online Privacy Protection Rule* [hereinafter *COPPA FAQ*], Question 6 ("What types of online transmissions does COPPA apply to?"), www.ftc.gov/privacy/coppafaqs.shtm.

25. Operators of PI-collecting sites must:

> Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information; … (c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance; (d) Not condition 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 in such activity; and (e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

16 C.F.R. § 312.3 (internal cross-references omitted).

26. 16 C.F.R. Part 312. We use "COPPA Rule" when referring specifically to the FTC's implementing regulations, but use "COPPA" both to refer to the statute itself and to the scheme generally where appropriate.

27. *See* Federal Trade Commission, *How to Comply with The Children's Online Privacy Protection Rule*, Nov. 1999**,** www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.shtm.

28. 16 C.F.R. § 312.5(b)(2). *See generally* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999), *available at* www.ftc.gov/os/1999/10/64fr59888.pdf [hereinafter *1999 COPPA Order*]; *see also COPPA FAQ* supra note 24, Question 32 ("How do I get parental consent?").

29. The four safe harbor programs are administered by the Children's Advertising Review Unit of the Council of Better Business Bureaus (CARU); the Entertainment Software Rating Board (ESRB); TRUSTe; and Privo. *See* Federal Trade Commission, *Safe Harbor Program*, www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html.

In a February 2007 report to Congress about the status of the law and its enforcement, the FTC said that no changes to COPPA were then necessary because the law had "been effective in helping to protect the privacy and safety of young children online."[30] In discussing the effectiveness of the parental consent verification methods authorized in the FTC's sliding scale approach, however, the agency acknowledged that "none of these mechanisms is foolproof."[31] The FTC attempts to distinguish these parental consent verification methods from other kinds of age verification tools in noting that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms."[32] This makes it clear that the FTC does not regard the methods the agency has prescribed for obtaining parental consent under COPPA as equivalent to strict age verification.

Although credit cards may seem the most robust tool for verifying parental consent (essentially, age verifying the parent), federal courts have found, in rejecting the constitutionality of COPA, that, "payment cards cannot be used to verify age because minors under 17 have access to credit cards, debit cards, and reloadable prepaid cards" and, although "payment card issuers usually will not issue credit and debit cards directly to minors without their parent's consent because of the financial risks associated with minors… there are many other ways in which a minor may obtain and use payment cards."[33]

B. "Collection": When Parental Consent is Required

COPPA requires that operators obtain verifiable parental consent "before any collection, use, and/or disclosure of personal information from children"—as well as for "any material change in the collection, use, and/or disclosure practices to which the parent has previously consented,"[34] subject to certain narrow exceptions.[35] Understanding how the COPPA Rule currently works and the pitfalls of COPPA expansion requires examining the three-pronged definition of "collection" created by the FTC, which COPPA itself left undefined.[36]

---

30. Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* at 1*,* Feb. 2007, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf [hereinafter *2007 COPPA Implementation Report*].

31. *Id*. at 13.

32. *Id*. at 12.

33. *Gonzales*, 478 F. Supp. 2d at 801. COPA would have prohibited the online dissemination of material deemed harmful to minors under 17 for commercial purposes, 47 U.S.C. § 231(a)(1), subject to a safe harbor for sites that made a "good faith" effort to restrict access by minors: "(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; (B) by accepting a digital certificate that verifies age; or (C) by any other reasonable measures that are feasible under available technology," 47 U.S.C. § 231(c)(1).

34. 16 C.F.R. § 312.5(a).

35. 16 C.F.R. § 312.5(c).

36. The FTC has provided three definitions of "collection":

> the gathering of any personal information from a child by any means, including but not limited to: (a) Requesting that children submit personal information online; (b) Enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they

1. Requests from Sites

Most obviously, the COPPA Rule considers "collection" to occur each time a PI-collecting site requests "that children submit personal information online."[37] This requirement generally minimizes the amount of data collected from children and ensures that parents control the collection of information from their children.

2. Enabling Sharing of Personal Information

Less intuitively, the COPPA Rule considers "collection" to occur when a PI-collecting site merely "enabl[es] children to make personal information publicly available… *except where* the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records."[38]

Unlike the first prong of "collection," consent is not required each time a communications tool is used to "make personal information publicly available", but merely for the child to gain access to the tool (*e.g.*, upon creation of a user account). Thus, the FTC intends to make parents gatekeepers over which sites their children join or participate in, rather than to give parents a veto right over every instance in which a child wants to share personal information (*e.g.*, by posting it to their profile or "wall" on a social networking site). Given the degree of interactivity on social networking sites, it is difficult to imagine how so granular a veto requirement could be feasibly implemented if COPPA were expanded.

What it means to make information "publicly available" is unclear. COPPA clearly requires consent before granting a child access to a site that would allow the child to "broadcast" personal information, such as by posting their name, photo, contact information, *etc*. such that the "public" can access that information, whether that means posting information to a social networking profile, on a website, or in a "public" chat room or message board (the latter two being the specific examples cited in COPPA and the COPPA Rule).[39] But does COPPA apply to communications that are not intended to be public? Would COPPA apply to a site that only allowed users to send "private" messages to each other? In short, how public is "public" enough that giving a child access to the underlying functionality would constitute collection? The FTC has never clearly answered these questions, but it has implied that it takes the "maximalist" view of what counts as collection: Allowing children to share personal information with *anyone*, even in one-to-one communications, constitutes "collection" subject to COPPA's parental consent requirement.[40] By contrast, the "minimalist" view would define

---

> are made public, and also deletes such information from the operator's records; or (c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.

16 C.F.R. § 312.2. *See also infra* at Section II.B.

37. 16 C.F.R. § 312.2 (definition of "collection").

38. *Id*.

39. 15 U.S.C. § 6501(4)(B)(iv-v) (definition of "disclosure"); 16 C.F.R. § 312.2 (definition of "collection").

40. In December 2007, the FTC added a question it its FAQ reflecting the agency's view that COPPA would require parental consent before allowing a child to send electronic greeting cards or forward items of interest to their friends. *COPPA FAQ supra note* 24, Question 44 ("My child-directed website wants to offer electronic post cards and the ability for children to forward items of interest on my site to their friends. Can I take advantage of

"collection" in terms of the capability to "publish" or "broadcast" personal information such that it becomes "available" to anyone with access to the PI-collecting site. Which view a court would accept, if presented with a challenge to COPPA, is beyond the scope of this paper, but the ambiguity is worth noting.[41]

However broad the definition of "publicly available," the FTC's definition of "collection" to include the enabling of communication by children that might result in the any of personal information was itself controversial when the FTC first wrote the COPPA rules. The FTC (again) took a maximalist view of "collection,"[42] overriding the objections of free speech advocates who argued that Congress intended "to place duties on those who collect information from children" (in the normal sense of "collection" contained in the first prong of the definition) rather than "to regulate children's behavior" or "limit children's ability to speak."[43] These advocates proposed a minimalist definition of "collection" as "gathering, by an operator, of personal information," such that merely providing functionality like chat rooms and message boards would not constitute collection unless the operator actually gleaned personal information from such fora.[44]

3. Online Tracking & Cookies

Finally, COPPA would consider collection to occur through the use of persistent identifiers such as cookies[45] if associated with individually identifiable information or "a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting."[46]

---

one of the email exceptions to parental consent?"). The FTC requires parental consent if users can "freely type messages in either the subject line of the e-card or in any text fields"—presumably, because this might lead to the sharing of personal information with the card's recipient. *See* Jim Dunstan, *E-cards and "Forward-to-a-Friend" Promotions: Not Kid Friendly Anymore*, www.gsblaw.com/practice/notableevents.asp?StoryID=1137185152008&groupID=21; *see also* Jim Dunstan, *FTC Issues Final Rules in CAN-SPAM Proceeding: Forward-To-A-Friend Promotion Mystery Solved*, www.gsblaw.com/practice/notableevents.asp?StoryID=17866132008&groupID=21.

41. The maximalist approach essentially reads the term "publicly available" out of the statute by construing collection to mean "available to anyone." Such a construction might, for example, violate the cannon of statutory interpretation against surplusage: "[T]he presence of statutory language 'cannot be regarded as mere surplusage; it means something.'" Chickasaw Nation v. United States, 534 U.S. 84, 97 (2001) (quoting Potter v. United States, 155 U.S. 438, 446 (1894)).

42. *1999 COPPA Order*, *supra* note 28, at 59,889-890.

43. Supplemental Comments of The Center for Democracy and Technology, The American Civil Liberties Union, and The American Library Association, filed in *Rulemaking to Implement the Children's Online Privacy Protection Act of 1998*, Aug. 25, 1999, at § I.B www.ftc.gov/privacy/comments/supplementalcdtacluala.htm.

44. *Id*. (emphasis original, indicating proposed addition to the FTC's rule as originally proposed).

45. 16 C.F.R. § 312.2 (definition of "collects or collection").

46. 16 C.F.R. § 312.2 (definition of "personal information").

C. COPPA's Place in an Evolving Landscape

In the decade since Congress enacted COPPA, the kinds of information-sharing functionality governed by the "publicly available" prong of collection have exploded in popularity. New interactive communications tools and methods, now generally referred to as "social networking" capabilities, are a key hallmark of the "Web 2.0" era.[47] Of course, they had their precursors even in 1998, but the examples of such tools included in COPPA and the initial COPPA rule reveal just how much the web has evolved: "Chat rooms" and "message boards" certainly still exist but they have largely morphed into today's social networking sites (*e.g.*, Facebook, Myspace), which would have been unrecognizable in 1998, while services like blogging and micro-blogging (*e.g.*, Twitter) would have been inconceivable. Today, more users feel comfortable making personal information more "publicly available" than ever before, broadcasting their every thought and action, and even their exact physical location,[48] for all the world to see.

The growing ubiquity of "Web 2.0" tools has two implications. First, the sites currently covered by COPPA are growing ever more limited in their functionality relative to the rest of the Internet, as discussed below.[49] For example, child-oriented sites must obtain verifiable parental consent before allowing children to send e-cards or use "Forward-to-a-Friend" functionality if the sites "permit the sender to enter her full name, her email address, or the recipient's full name" or "provide users with the ability to freely type messages in either the subject line of the e-card or in any text fields."[50] Second, even under the minimalist view of "publicly available," expanding COPPA's age scope would affect far more websites today than it would have 11 years ago, because the functionality that constitutes "collection" (under the second prong of that term's definition) is now pervasive.

III. Does COPPA Really Work?

Before addressing the many challenges associated with COPPA 2.0 proposals, one must ask the critical—but ignored—threshold question: Is "COPPA 1.0" really working? To answer this question, one must first decide what COPPA 1.0 is supposed to accomplish. The original goals of COPPA, as expressed by its Congressional sponsors, were to:

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of

47. Tim O'Reilly, *What Is Web 2.0?: Design Patterns and Business Models for the Next Generation of Software*, Sept. 30, 2005, www.oreillynet.com/lpt/a/6228.

48. See, e.g., Google Latitude, www.google.com/latitude/intro.html; loopt, www.loopt.com; Pelago, http://pelago.com.

49. *See infra* at Section III.A.

50. Absent such sharing, the FTC allows child-oriented sites to use COPPA's exception for one-time communications, found at 16 C.F.R. § 312.5(c). *See supra* note 40.

> identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[51]

Thus, as its name implies, COPPA is first and foremost about protecting the privacy of children. COPPA's primary means for achieving this goal is enhancing parental involvement or, as the FTC has put it, "provid[ing] parents with a set of effective tools… for becoming involved in and overseeing their children's interactions online."[52] However admirable, "protect[ing] the safety of children" is merely an *indirect* goal of COPPA—something to be achieved through the means of enhancing parental involvement (COPPA's *direct* goal). The FTC has attempted to blur this distinction, elevating child protection to a direct goal of COPPA.[53] Indeed, this was the primary reason the FTC adopted the maximalist definition of "collection" to include enabling communication (rather than direct gathering of personal information by operators), over-ruling free speech concerns.[54]

The FTC claims COPPA "has provided a workable system to help protect the online safety and privacy of the Internet's youngest visitors."[55] Indeed, many of those advocating expansion of COPPA do so on the grounds that COPPA makes children safer online from sexual predators. What these advocates fail to acknowledge is that, to the extent COPPA has enhanced child safety—indeed, to the extent that COPPA can be effectively administered at all—it is because of the unique circumstances of the under-13 age bracket and the PI-collecting sites that have evolved to serve that community. In particular:

1. The functionality of child-oriented sites is usually tightly limited: They are closed, walled gardens;
2. Many smaller websites catering to children charge a fee for admission—even as fee-based models have withered away on the rest of the Internet; and
3. There are relatively few sites that cater exclusively to the under-13 crowd, which may be an unintended consequence of COPPA itself.

---

51. 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

52. *2007 COPPA Implementation Report, supra* note 30, at 28.

53. The FTC has carefully—or perhaps simply carelessly—edited Congress's original statement of purpose: Where Congress had originally declared that COPPA was intended "*to enhance parental involvement* to help protect the safety of children [online]," 144 Cong. Rec. S11657 (emphasis added), the FTC has declared that COPPA was intended "to protect the safety of children [online]." *2007 COPPA Implementation Report, supra* note 30, at 3.

54. The FTC based its adoption of the maximalist view of "collection" by noting that:

> children's use of chat rooms and bulletin boards that are accessible to all online users present the most serious safety risks, because it enables them to communicate freely with strangers. Indeed, an investigation conducted by the FBI and the Justice Department revealed that these services are quickly becoming the most common resources used by predators for identifying and contacting children.

1999 COPPA Order, *supra* note 28, at 59,890 (internal citations omitted). *See also supra* at 11 and note 43.

55. *2007 COPPA Implementation Report, supra* note 30, at 28.

Each of these factors is discussed below, as relates to COPPA's perceived goals.

A. Child-Oriented Sites Limit Functionality

Child-oriented sites typically have very limited functionality: In essence, their operators intentionally "cripple" the sort of functionality found in most PI-collecting sites (especially social networking sites) geared toward older users. *That fact alone makes COPPA-covered sites far less likely to be subject to fraudulent entry or dangerous interactions*: Why would an adolescent or an adult predator ever want to gain access to a site that offers little more than drop-down menus and a few buttons to click on when interacting with others?

The primary reason that children are likely safer in those environments probably has less to do with COPPA's parental consent requirements and much more to do with the fact that most of the PI-collecting sites covered by COPPA are tightly controlled and highly moderated walled gardens with very limited functionality—a sort of "Junior Internet."

B. Child-Oriented Sites Charge Fees

While most Internet content and services are now "free" (*i.e.*, advertising-supported),[56] many child-oriented PI-collecting sites charge admission fees. There are several reasons they do so:

- "[R]equiring a parent to use a credit card in connection with a transaction" is among the methods for obtaining verifiable parental consent in the FTC's sliding scale.[57] The FTC requires that an operator charge some fee so that the credit card will be verified by its issuer and "because, through receipt of a monthly statement, the parent is given additional notice that the transaction occurred and has an opportunity to investigate any suspicious activity and revoke consent."[58]
- Commercial child-oriented sites must somehow recoup the costs of obtaining verifiable parental consent—estimated in 2005 at more than $45 per child.[59] Because COPPA limits operators' ability to effectively target advertising to children, thereby reducing the value of advertising inventory on PI-collecting sites, they usually must rely on direct fees.
- Many child-oriented sites rely heavily on constant human moderation and oversight, which necessitates a method of funding those workers.

---

56. *See, e.g.,* Chris Anderson, *Free! Why $0.00 Is the Future of Business*, Wired, Feb. 25, 2008, www.wired.com/techbiz/it/magazine/16-03/ff_free. The most notable exception to this rule is Massively Multiplayer Online games such as World of Warcraft, which are also potentially subject to COPPA.

57. 16 C.F.R. § 312.5(b)(2).

58. *See COPPA FAQ*, *supra* note 24, Question 33 ("I would like to get consent by collecting a credit card number from the parent, but I don't want to engage in a transaction. Is this ok?").

59. *See* Comments of Parry Aftab, Request for Public Comment on the Implementation of COPPA and COPPA Rule's Sliding Scale Mechanism for Obtaining Verifiable Parental Consent Before Collecting Personal Information from Children at 2, June 27, 2005, www.ftc.gov/os/comments/COPPArulereview/516296-00021.pdf [hereinafter *Aftab Comments*].

- It is easier for child-oriented sites to continue charging small fees once they have a credit card on file (something most sites never accomplish) and because there is relatively less competition in the child-oriented marketplace than in the Internet generally.

Importantly, the more a site charges for access, the more likely it is that the parent or guardian pays attention to what their child is doing on that site. The hassle for parents of having to pay a fee gets parents thinking, and talking to their kids, about those sites, argues Denise Tayloe of Privo, one of the four FTC-approved providers of COPPA safe harbor age verification services.[60]

However, Tayloe has noted that one of the problems associated with the current COPPA regime is that "Children quickly learned to lie about their age in order to gain access to the interactive features on their favorite sites. As a result," she notes, "databases have become tainted with inaccurate information and chaos seems to be king where COPPA is concerned."[61] The FTC, well aware that blocking access to children under 13 could simply encourage them to lie about their age, requires operators to "design [their] age collection input screens in a manner that does not encourage children to provide a false age in order to gain access to [their] site."[62] In particular, the FTC recommends "using a temporary or a permanent cookie to prevent children from back-buttoning to enter a different age."[63] But if children can learn to lie about their age, they can probably learn to delete cookies, too—since cookie deletion is a privacy feature now common in every browser.[64]

Despite these problems, Tayloe falls back on the original justification of COPPA: increasing parental involvement. Even though "there is no perfect solution" and it is not possible to completely "stop a child from lying and putting themselves at risk," Tayloe believes that COPPA "provides a platform to educate parents and kids about privacy."[65] Providing a platform to educate parents and kids about online privacy or safety is certainly important, but there are other ways to do this besides imposing strict age verification mandates. Educational initiatives and public service announcements, for example, could also encourage greater parent-child interaction. Indeed, the courts have concluded that the First Amendment *requires* the government to utilize such educational initiatives as "less restrictive" alternatives to age verification technologies in other contexts.[66]

While we don't really have any idea what level of parent-child interaction COPPA incentivizes, or how many children (or adults) are able to gain access to PI-collecting sites under false pretenses, the key operational assumption on which COPPA rests is that by creating an added

---

60. Denise Tayloe, *It's Time to Comply with COPPA*, The Privacy Advisor, Vol. 6, No. 10, Oct. 2006, at 5.

61. *Id*.

62. *See COPPA FAQ*, *supra* note 58, Question 39 ("Can I block children under 13 from my general audience website?").

63. *Id*.

64. Adam Thierer, Berin Szoka & Adam Marcus, The Progress & Freedom Foundation, *Privacy Solutions*, PFF Blog, Ongoing Series, http://blog.pff.org/archives/ongoing_series/privacy_solutions.

65. E-mail from Denise Tayloe to Adam Thierer (Mar. 15, 2007) (copy on file with author).

66. *See infra* at VI.A.3.

economic hurdle or barrier to entry (in the form of entry fees or the hassle of filling out paperwork or forms), COPPA gets some—maybe even most—parents to put more thought into what their kids are doing online, and that in turn somehow improves online child safety.

However useful COPPA might be in enhancing parental involvement, it does *not* necessarily mean that children are operating in perfectly "secure" or "verified" environments. COPPA wasn't primarily put on the books to prevent "bad guys" from interacting with children online; it was about minimizing the collection of children's personal information and giving parents control over collection of information from their children.[67] Thus, COPPA does not require excluding older users from child-oriented sites, some websites indeed may try to do so, building on COPPA's required age verification system, because of market demand from parents to exclude sexual predators. Of course, age verification is hardly fool-proof for either kids or adults. So, to the extent some "bad guys" are getting on those sites under false pretenses, both children and parents may be lulled into to a false sense of security after they are told the site is COPPA-verified—whether or not the site actually attempts to exclude older users and regardless of how effective the site may be in doing so. This may actually *increase* the danger of predation to children.[68]

C. Does COPPA Encourage Consolidation or Limit Competition?

As noted above, there are significant costs associated with the verifiable parental consent methods that PI-collecting sites must implement to comply with COPPA. If we are to fully understand the experience of COPPA as a regulatory model, we must consider the extent to which COPPA may have had the unintended consequence of limiting choice and competition by driving increased consolidation in the marketplace for child-oriented sites and services online—

---

67. *See supra* at 16.

68. Internet security expert John Cardillo argues that even COPPA-compliant sites are vulnerable:

> During an analysis of the security processes of certain sites we tested Imbee's. Our security team was able to create several fake children. More troubling was the inconsistency of the information used to do so. We used a fake name for the parent, a different fake name created for the Yahoo! e-mail account used at registration, and my credit card info (because the name on the CC is irrelevant). Fictional child, and three fake identifiers on supposedly the same adult. Not one red flag was raised, and we were allowed onto the site without a problem. Our team was able to do this multiple times. Had we been a real bad guy, we could have, at any time, chatted with other kids on the site as a child. One of several different children actually. Not only isn't it a security solution, it's downright dangerous.

E-mail from John J. Cardillo to Adam Thierer (March 11, 2007) (copy on file with author). Cardillo's findings thus make it clear how real predators intent on doing harm to children could exploit age verification processes designed to exclude adults from a supposedly "teens-only" site (just as predators already do with sites supposedly limited to kids under 13). Indeed, because many predators have children of their own, they might use this approach to obtain an ID for their own kids and then go online under their child's name to prey on other children. The fiction that all users of a site are "verified" creates a false sense of security—a serious problem for child safety. As Cardillo has noted elsewhere, predators who create a "pedophile passport" could operate freely in supposedly "safe and secure" environments. *See* Adam Thierer, The Progress & Freedom Foundation, *Age Verification for Social Networking Sites: Is It Possible? Is It Desirable?*, Progress on Point 14.8, May 2007, at 6, www.pff.org/issues-pubs/pops/pop14.8ageverificationtranscript.pdf.

a question the FTC should consider answering. As early as 2001, even some Congressmen recognized this "unintended consequence" of COPPA in Congressional hearings on privacy.[69]

Of course, it could be the case that there are other reasons that there are relatively few sites catering exclusively to children. Nonetheless, as discussed below, it's worth considering how expanding COPPA might lead to more consolidation in the marketplace or how it discourages greater entry by smaller "mom-and-pop" sites that could cater to children. As noted by Parry Aftab, Executive Director of the children's advocacy group Wired Safety, "COPPA wasn't responsible for the demise of these sites, but when combined with the other factors [it] tipped the balance."[70] She concludes, appropriately:

> It is crucial that at this tentative stage for the kids Internet industry we don't do anything to make its survival more difficult. We should be looking at easy to encourage safer communities for preteens and innovations to help create fun, entertaining and educational content for kids online.[71]

IV. What if COPPA Were Expanded to Cover Adolescents?

However effective COPPA might be in fulfilling its purposes, and whatever its unintended consequences, the COPPA Rule's requirements are *relatively* easy for the private sector to implement and for the government to enforce because, as mentioned, they apply only to the collection of information about children under 13 by commercial operators only when (i) the operator's PI-collecting Site or service is "directed to children" or (ii) the operator has actual knowledge that they are collecting personal information from a child. But how well would the COPPA approach "scale up" to the 13-17 age bracket?

The key practical difficulty in implementing a COPPA 2.0 system for adolescents is in the anonymity inherent in the technical architecture of the Internet. To quote a memorable cartoon from *The New Yorker* of all time: "On the Internet, nobody knows you're a dog."[72] Because website operators generally do not know who is accessing their site, requiring any special treatment of minors (*e.g.*, parental consent prior to the collection of personal

---

69. Rep. Billy Tauzin (R-LA) noted that COPPA "has now forced companies to discontinue a number of products targeted toward children" and asked "If we end up forcing private companies and nonprofits to eliminate beneficial products such as crime prevention material, have we done a good thing? If teen-friendly sites, those that totally respect the privacy of the users stop offering e-mail services to children, is that a good thing? *An Examination Of Existing Federal Statutes Addressing Information Privacy: Hearing of the House Committee On Energy And Commerce*, 107th Cong. 6 (April 3, 2001) (statement of Rep. Tauzin.), *available at* http://republicans.energycommerce.house.gov/107/action/107-22.pdf.

70. *Aftab Comments*, *supra* note 59, at 3.

71. *Id.*

72. Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, The New Yorker, July 5, 1993 at 61, available at www.unc.edu/depts/jomc/academics/dri/idog.html (cartoon of a dog, sitting at a computer terminal, talking to another dog).

information, access to the child's user profile) is tantamount to requiring age-verification of all users.[73]

Because "child-oriented" websites are generally easy to define and are very rarely used by adults, COPPA 1.0's age verification mandate has not significantly impacted the free speech rights of adults. But it is *far* more difficult to define a class of "adolescent-oriented" websites (as proposed in New Jersey) that are not also used by significant numbers of adults. Indeed, the Illinois bill does not even attempt to do so, defining its scope not in COPPA's "directed at" terms but purely in terms of site functionality.[74] In this sense, the Illinois bill is more restrictive than the New Jersey bill, since it would apply to sites with a certain functionality regardless of to whom they are "directed at." On the other hand, the New Jersey proposal is far more sweeping, since it applies to any site that collects user information if the site is "directed at" adolescents.[75] Whichever bill might ultimately affect more websites, the practical result of both COPPA 2.0 proposals is the same: They would, without explicitly saying so, require age verification of a large numbers of adults. This raises profound First Amendment concerns—particularly about the right of Americans to speak and receive information anonymously online.[76]

V. The Differences Between Children (0-12) & Adolescents (13-17)

Before examining these First Amendment concerns (which are more directly apparent in the case of the Illinois proposal), one must ask how they arise in the case of the more complicated New Jersey proposal, which applies to PI-collecting sites "directed at" adolescents.[77] This

---

73. Of course, the COPPA's second prong of age-verification requirement applies only when the website operator has "actual knowledge" that the user is a minor. *See supra* at 7 & note 22.

74. The Illinois Bill defines a "social networking site" as:

> an Internet website containing profile web pages of the members of the website that include the names or nicknames of such members, photographs placed on the profile web pages by such member, or any other personal or personally identifying information about such members and links to other profile web pages on social networking websites of friends or associates of such members that can be accessed by other members or visitors to the website. A social networking website provides members of or visitors to such website the ability to leave messages or comments on the profile web page that are visible to all or some visitors to the profile web page and may also include a form of electronic mail for members of the social networking website.

SNWARA, supra note 11, § 5. This definition seems almost tailor-made for MySpace and Facebook: The second sentence of the definition would exclude sites like LinkedIn, which includes profiles but does not allow users to post public comments on other users' profiles. While this focus on specific site functionality seems to differ from COPPA's approach, in fact it does little more than apply COPPA's second definition of "collection" as "Enabling children to make personal information publicly available." *See* 16 C.F.R. § 312.2 (definition of "collection"); *see also supra* at 8.

75. *See supra* note13.

76. Adam Thierer, The Progress & Freedom Foundation, *USA Today, Age Verification, and the Death of Online Anonymity*, PFF Blog, Jan. 23, 2008, http://blog.pff.org/archives/2008/01/usa_today_doesn.html.

77. Like COPPA, New Jersey's AOPPA bill also applies to cases of actual knowledge that an operator is collecting personal information from an adolescent. *See supra* note 13.

examination reveals the fundamental flaw in *any* attempt to extend COPPA to cover adolescents: COPPA 1.0 works only because of the unique characteristics of the under-13 age bracket.

A. Subjective Assessments About Intended Audiences Are Significantly Easier for Children than for Adolescents

In determining whether a PI-collecting Site or service is "directed at children," the FTC considers the site or service's "subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children…. and whether a site uses animated characters."[78] The following excerpts from FTC complaints illustrate how the agency has applied these criteria:

> The … subject matter [of www.lilromeo.com] is Lil' Romeo, a twelve-year-old recording artist who "enjoys 'just being a regular kid.'" The website features content directed to children such as an animated game in which the player helps Lil' Romeo save an elementary school from aliens by answering simple math and history questions. The website also features music and lyrics from Lil' Romeo's album "Game Time," which is "about having fun, and also about, you know, kids[']things…"[79]

And:

> Defendant operates the www.etch-a-sketch.com website, which provides information about its toys, including the "Etch A Sketch" drawing toy. The subject matter, visual content, and language of this website are directed to children under the age of 13. For example, the site features a cartoon character named "Etchy" - an Etch A Sketch sporting sunglasses, purple hair and legs. Etchy invites visitors to play "cool games," such as drawing with an online Etch A Sketch, finding hidden numbers, letters and shapes, and coloring pictures of Etchy and friends. The site also contains an "interactive story" titled, "Etchy Goes to a Birthday Party."[80]

The FTC settled both cases with consent decrees—like, apparently, all the FTC's COPPA enforcement actions.[81] These examples demonstrate that subjective standards *can* sometimes work reasonably well in certain contexts. As Justice Potter Stewart famously said of obscenity, "I know it when I see it."[82] The same could probably be said, in many cases, about what

---

78. 16 C.F.R. § 312.2 (definition of "Website or online service directed to children").

79. U.S. v. UMG Recordings, Inc., Civil Action No. CV-04-1050, Complaint at 4-5 (C.D. Ca. 2004), www.ftc.gov/os/caselist/umgrecordings/040217compumgrecording.pdf.

80. U.S. v. The Ohio Art Company, Complaint, ¶ 12 (N.D. Oh. 2002), www.ftc.gov/os/2002/04/ohioartcomplaint.htm.

81. *See* Federal Trade Commission, *Children's Privacy Enforcement Cases*, www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html (including a consent decree for each case).

82. Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

constitutes child-oriented content; and this approach seems to have worked well enough for the FTC's COPPA enforcement efforts. But how well, if at all, would such a standard work in determining the scope of COPPA 2.0 proposals (like New Jersey's) that retain COPPA's requirement that a site be "directed at" a certain audience when that audience is not children (0-12) but adolescents (13-17)?[83]

Any regulatory system that, like COPPA, rests on age stratification inevitably requires the drawing of arbitrary boundaries. But ultimately, *some* age must be chosen. Whatever the differences between 12 and 13, the differences between 12 (COPPA's ceiling) and 17 (the ceiling established in some COPPA 2.0 measures) are significant. Although the original version of the COPPA legislation would have required "reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information" for kids 13-16, the legislation never required verifiable parental consent for minors above 12.[84] The FTC explains Congress's rationale for this distinction as follows:

> Congress and industry self-regulatory bodies have traditionally distinguished children aged 12 and under, who are particularly vulnerable to overreaching by marketers, from children over the age of 12, for whom strong, but more flexible protections may be appropriate. In addition, distinguishing adolescents from younger children may be warranted where younger children may not understand the safety and privacy issues created by the online collection of personal information.[85]

Thus, it appears that Congress was simply following a long-standing distinction based on the cognitive capabilities of children under 13. But whether anyone realized it at the time, this distinction has proved essential for the administration of COPPA as a statute that defines its scope by the audience to which sites are "directed." Whenever the "tipping point" in cognitive capabilities occurs, the age of 13 roughly corresponds to an important point of departure in psychological growth between "childhood" and "adolescence."

This moment was best described two thousand years ago by the Apostle Paul of Tarsus, when he wrote, "When I was a child, I spake as a child, I understood as a child, I thought as a child:

---

83. While New Jersey's proposal retains this approach, hewing closely to COPPA's current structure, *see supra* note 13 and accompanying text , Illinois's proposal drops the concept and simply applies to all sites with certain social networking functionality, *see supra* note 11.

84. *See supra* note 14 and associated text.

85. *COPPA FAQ*, *supra* note 58, Question 8 ("Why does COPPA apply only to children under 13? What about protecting the online privacy of teens?"), www.ftc.gov/privacy/coppafaqs.shtm. The FTC also reminds companies:

> websites' information practices regarding teens and adults are subject to Section 5 of the FTC Act, which prohibits unfair or deceptive acts and practices. See Staff Opinion Letter to Center for Media Education (July 15, 1997) for guidance on how Section 5 applies to information practices involving teens. In addition, recent concern about the risks of child participation on social networking websites led the FTC to issue a set of safety tips for social networking. *See* "Social Networking Sites: A Parents' Guide" (September 2007), *available at* www.ftc.gov/opa/2006/05/socialnetworking.shtm; *see also* www.onguardonline.gov/docs/onguardonline_socialnetworking.pdf.

but when I became a man, *I put away childish things*."[86] Paul equated what we think of as "adolescence"—a profoundly modern invention[87]—with adulthood. Paul had no more conception of "adolescence" than did Shakespeare, who—like Congress with COPPA—chose thirteen as the age of Juliet, his greatest star-crossed lover.[88] But Paul offered perhaps the best reason why COPPA's scope ends at thirteen: this is the roughly point at which minors begin to shun "childish things"—say, losing interest in Club Penguin in favor of more "grown-up" sites like MySpace or Facebook. If one has to choose a clear bright line rule as to when, on average, that shift occurs, 13 seems to be about as accurate as any. (Indeed, modern Jews—like the Jewish Paul before them—continue to recognize this as the threshold of maturity by generally holding a Bar Mitzvah for boys at age 13, and a Bat Mitzvah ceremony for girls at age 12.[89]) This is less a question of how much protection minors of any particular age require, and more a question of when their interests change: At about this age, adolescents begin to share interests with adults in ways that children 12 and below do not; if left to their own devices, adolescents would spend far more time on "general audience"[90] websites than would children. Thirteen is probably about the point at which this transformation begins to accelerate. But regardless of precisely when it happens, it should be apparent that the sites favored by adolescents 13 and over will be difficult to distinguish as "adolescent-oriented" because they are rarely, if ever, as thoroughly dominated by adolescents as "child-oriented" sites are by children 12 and under. This problem gives rise to the significant constitutional concerns raised by COPPA 2.0 proposals.

B. The Difficulties of Empirical Assessments about Intended Audiences

If the subjective "I know it when I see it standard" is not so easily applied for determining what constitutes adolescent-oriented PI-collecting sites, the alternative under the FTC's COPPA rules is to examine "competent and reliable empirical evidence."[91] Could demographic data about a

---

86. *The First Epistle of Paul the Apostle to the Corinthians* 13:11 (King James), *available at* www.bartleby.com/108/46/13.html (emphasis added).

87. Sociologist Rowan Wolf explains:

> [F]or much of the history of human society, there has not really been the concept of "childhood" as we know it today. Once a child was able to speak and eat on its own, it was essentially considered a miniature adult capable of participating in a limited way in the survival of the family. Once "children" hit puberty, they were considered adults, though they might not take on adult roles until they formed their own family. There was no concept of adolescence…. Children went from "miniature adults" expected to act like adults but without the rights of adults, to a carefree, dependent period of exploration and learning. When we look at the expectations of "teenagers," we define this as a rebellious period of individuation. We simultaneously expect adolescents to act like adults and rebel from them at the same time. This is a period where people are sexually mature, but socially and economically dependent.

Age Stratification, Sept. 2005, www.srwolf.com/wolfsoc/articlearchives/2008/11/age_stratification.html.

88. *See, e.g., The Invention of Adolescence,* Psychology Today, Jan./Feb. 1995, www.psychologytoday.com/articles/pto-19950101-000024.html.

89. *See, e.g., Bar Mitzvah, Bat Mitzvah and Confirmation*, Judaism 101, http://www.jewfaq.org/barmitz.htm.

90. The term "general audience" is commonly used instead of "adult-oriented" for content that is not directed at children.

91. 16 C.F.R. § 312.2 (definition of "Website or online service directed to children").

site's membership provide sufficiently clear guidance about the scope of a law that (like New Jersey's proposal) retains COPPA's current "directed at" approach?[92]

The FTC has never addressed the difficult question of setting a minimum threshold of child membership/participation in a site above which the site would be considered "directed at children:" Not one of the complaints brought by the FTC under COPPA cites demographic evidence. Because, as discussed above, child-oriented websites tend to exist in a virtually distinct "Junior Internet," with little overlap between adults and children, and because many parents use technological controls to keep their children (but not their adolescents) within this Junior Internet, it is hardly surprising that the FTC has never answered this question: Subjective criteria are generally sufficient to identify child-oriented sites, and those sites are likely to be used overwhelmingly by children or young adolescents with very little adult participation.

But as discussed above, few of the websites frequented by adolescents are dominated so overwhelmingly by adolescents as children dominate the membership of the Junior Internet to which COPPA currently applies. Instead, adolescents participate in many of the same PI-collecting sites used by adults, as demonstrated by the following sample of some of the more popular Web 2.0 sites, including demographic estimates:

Exhibit 1: Popular Web 2.0 Sites[93]

Site Name	Unique U.S. Users	Annual U.S. Page Views	% of Users Under Age 18
myyearbook.com	2,000,000	860,000,000	50.00%
bebo.com	2,400,000	340,000,000	35.00%
nickjr.com	2,400,000	210,000,000	31.67%
myspace.com	67,000,000	43,000,000,000	28.36%
photobucket.com	25,000,000	1,300,000,000	26.80%
movie6.net	1,100,000	24,000,000	26.36%
fanpop.com	1,100,000	16,000,000	21.82%
xanga.com	1,600,000	82,000,000	20.00%
tagged.com	3,500,000	1,100,000,000	19.71%
zango.com	2,900,000	21,000,000	17.93%
aol.com	37,000,000	4,000,000,000	16.49%
hi5.com	2,800,000	870,000,000	15.00%
facebook.com	74,000,000	30,000,000,000	12.16%
yahoo.com	140,000,000	36,000,000,000	11.43%
friendster.com	1,600,000	490,000,000	11.25%
wordpress.com	23,000,000	300,000,000	10.43%
gametrailers.com	1,200,000	50,000,000	10.00%
flickr.com	21,000,000	1,000,000,000	9.52%

92. *See supra* note 13.

93. Data obtained from Google Ad Planner on Mar. 1, 2009, https://www.google.com/adplanner/planning (by dividing "UV users" for the 0-17 "audience" by "UV users" for the entire population).

So would some of these sites be considered "adolescent-oriented" even though most of their users are actually adults? Perhaps not in New Jersey (depending on the circumstances of any particular site),[94] but this is essentially what the Illinois bill requires:[95] The approximately 88% of Facebook's users 18 and above must be age verified for the sake of obtaining parental consent for the 12% under 18. This example is apt, because 12% happens to coincide with the estimated percentage of American Internet users under 18: 12.6% or 28 million Americans.[96]

C. Possible Reactions to COPPA 2.0's Uncertain Scope

Of the top 250 sites ranked by audience reach, only a handful stand out as being obviously child-oriented, such as cartoonnetwork.com and nick.com (Nickelodeon). A number of leading social networks top the list and many, if not most, of these sites require the sharing of *some* personal information (if only an e-mail address) for full functionality. But how would *any* of these operators—let alone the millions of sites in the "Long Tail" of Internet content—determine whether they would be considered adolescent-oriented? By the same token, how should a legislator following Illinois's approach (defining the scope of the COPPA 2.0 law in terms of site functionality) decide which features should trigger age verification requirements?

To the extent PI-collecting Site operators might be unsure whether a COPPA 2.0 age verification mandate would apply to them, they would likely take one of the following steps to minimize their potential liability.

1. Trying to Block All Adolescents

Of course, since PI-collecting Site operators do not know which would-be users are minors without an age verification system (and perhaps not even then!), the most they could do would be to *claim* that they block access by adolescents. Websites can certainly try to block users who initially admit to being under 18 from trying to register again for the site.[97] But this approach is only effective to the extent that adolescents are naïve enough to admit their true age in the first place and not to know how to circumvent whatever system the operator has in place for preventing users from trying to register for the site after initially being blocked—which should be relatively simple to do (*e.g.*, by deleting cookies from the site).

2. Avoiding Actual Knowledge

Some PI-collecting Site operators may give up on the "directed at" prong and try to avoid gaining "actual knowledge" that a user is under 18 simply by ceasing to ask for age information upon the creation of a user account—or perhaps by no longer requiring the creation of user accounts altogether. But this is a dangerous gamble because, if a site is ultimately found to be "adolescent-oriented," *not* asking for age upon sign-up might be considered a serious violation

94. *See supra* note 13 and at 17.

95. *See supra* note 74.

96. Data obtained from Google Ad Planner on Mar. 1, 2009, https://www.google.com/adplanner/planning (by limiting age to 0-17).

97. *See supra* at 29.

in itself.[98] This "Catch-22" places site operators in a difficult and legally precarious position—especially significant smaller site operators trying to raise funding.

Other operators may reduce human moderation of their site in order to avoid situations in which an employee might learn that a user is under 18 *(e.g.*, by reading their comments or profile). This is precisely the sort of perverse incentive that Congress attempted to avoid in passing Section 230 of the Communications Decency Act of 1996, which fully immunized online intermediaries from liability even if they made "good Samaritan" efforts to self-police their sites for objectionable content.[99] (The FTC has already created this perverse incentive under COPPA, but given the demand among parents for heavy moderation on child-oriented sites, COPPA's perverse incentive may have had little effect.[100]) Thus, COPPA 2.0 proposals could lead to *less* protection for minors, not more, by discouraging site operators from "chaperoning" interaction on their sites. [101]

3. Age-Verifying *All* Users

COPPA 2.0's greatest threat is that large numbers of PI-collecting Site operators would be—or would feel—compelled to require age-verification of large numbers of adults as users. There is currently no age verification requirement other than COPPA, which affects adults only to the extent that parents need to establish their parental relationship to their kids. But COPPA affects few other adults because few adults want to use child-oriented PI-collecting sites like Disney's Club Penguin. COPPA 2.0 proposals would either *directly* require age verification of all adults who wanted to use "social networking sites" (as proposed in Illinois) or *indirectly* require much the same thing by mandating age verification for "adolescent-oriented sites" (as proposed in New Jersey). Indeed, this may be precisely what some COPPA 2.0 advocates want, since they may envision it as the only way to make the Internet truly "safe" for adolescents.

But few proponents would make such a goal explicit, for they know that such a "scaled-up" COPPA would essentially converge with COPA as a broad age verification mandate. As noted below, this highlights the First Amendment implications of trying to turn COPPA into something it was not designed to be: not merely a tool for enhancing parental involvement and kids' privacy, but a broad mandate for child safety.

---

98. For example, the amount of a penalty imposed on an operator deemed to be in violation would depend on "Respondent's good faith" and "The deterrent effect of the penalty action." 16 C.F.R. § 1.67(b) & (d).

99. "No provider or user of an interactive computer service shall be held liable on account of … any action taken to enable or make available to information content providers or others the technical means to restrict access to material … material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable…." 47 U.S.C. § 230(c)(2).

100. *See COPPA FAQ*, *supra* note 58, Question 41(b) ("What happens if a child visits a chat room or creates a blog and announces his or her age?"). The FTC answers: "You may be considered to have actual knowledge with respect to that child if someone from your organization sees the post, or if someone alerts you to the post (for example, a concerned parent who learns that his child is participating on your site). However, if no one in your organization is aware of the post, then you may not have the requisite actual knowledge under the Rule." *Id*.

101. *See infra* at 30.

VI. The First Amendment Implications of Broad Age Verification Mandates

Both COPPA and COPA rest on a stratification of users by age, but the approach of the two laws is very different: While COPPA requires age verification if content is "directed at" minors under age 13, COPA would have required that *all* website operators restrict access to material deemed "harmful to minors" by minors under the age of 17 and therefore requires age verification of *all* users who attempt to access such content (in order to identify minors). COPPA is focused on certain kinds of potentially harmful *contacts*[102] while COPA is focused on potentially harmful *content*.[103]

But by expanding the age range of COPPA to include adolescents, COPPA 2.0 proposals essentially converge with COPA, reaching the same practical consequence: age verification mandates for large numbers of adults *as users* (not as parents). Only the scope of sites covered by the laws is different: under COPA, sites deemed "harmful to minors," and, under COPPA 2.0, adolescent-oriented or certain social networking sites. Thus, to the extent that COPPA 2.0 proposals require age verification of adults, they would be subject to constitutional attacks similar to those against COPA. But COPPA 2.0 proposals would also burden the rights of adults to communicate with adolescents and the free speech rights of adolescents.

Finally, the fact that COPPA (like COPA) applies only to commercial sites would do little to protect it from constitutional attack, because in a world of user-generated content, the commercial nature of a site has little to do with the commercial/non-commercial nature of the speech carried on it. For example, obviously commercial sites like MySpace and Facebook serve as platforms for a wide variety of not-for-profit and political communications.

A. First Amendment Rights of Adults

After a decade-long court battle over the constitutionality of COPA, the U.S. Supreme Court in January 2009 rejected the government's latest request to revive the law, meaning it is likely dead.[104] Three of the key reasons the courts struck down COPA would also apply to COPPA 2.0 proposals.

1. Anonymous Speech Rights of Adults

COPA burdened the speech rights of adults to access information subject to age verification requirements, both by making speech more difficult and by stigmatizing it. In 2003, the Third Circuit noted that age verification requirements "will likely deter many adults from accessing restricted content, because many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to

---

102. *See supra* at 9.

103. COPA makes it illegal to "knowingly … make[] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." 47 U.S.C. 231.

104. *See* Adam Thierer, The Progress & Freedom Foundation, *Closing the Book on COPA*, PFF Blog, Jan. 21, 2009, http://blog.pff.org/archives/2009/01/closing_the_boo.html. *See also* Alex Harris, *Child Online Protection Act Still Unconstitutional*, http://cyberlaw.stanford.edu/packet/200811/child-online-protection-act-still-unconstitutional.

access is sensitive or controversial."[105] In 2008, in striking down COPA for the third and final time, the Third Circuit approvingly quoted the district court, which had noted that part of the reason age verification requirements deterred users from accessing restricted content was "because Internet users are concerned about security on the Internet and because Internet users are afraid of fraud and identity theft on the Internet."[106] The district court had held that:

> Requiring users to go through an age verification process would lead to a distinct loss of personal privacy. Many people wish to browse and access material privately and anonymously, especially if it is sexually explicit. Web users are especially unlikely to provide a credit card or personal information to gain access to sensitive, personal, controversial, or stigmatized content on the Web. As a result of this desire to remain anonymous, many users who are not willing to access information non-anonymously will be deterred from accessing the desired information.[107]

The Supreme Court has recognized the vital importance of anonymous speech in the context of traditional publication:

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Great works of literature have frequently been produced by authors writing under assumed names. Despite readers' curiosity and the public's interest in identifying the creator of a work of art, an author generally is free to decide whether or not to disclose his or her true identity. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[108]

By imposing broad age verification requirements, COPPA 2.0 would restrict the rights of adults to send and receive information anonymously just as COPA did. If anything, the speech burdened by COPPA 2.0 deserves *more* protection, not less, than the speech burdened by COPA: Where COPA merely burdened access to content deemed "harmful to minors" (*viz*., pornography), COPPA 2.0 would burden access to material by adults as well as minors not

---

105. American Civil Liberties Union v. Ashcroft, 322 F.3d 240, 259 (3d Cir. 2003) (*ACLU II*).

106. American Civil Liberties Union v. Ashcroft, 534 F.3d 181, 196 (3d Cir. 2008) (*ACLU III*) (*Gonzales*, 478 F. Supp. 2d 775 at 806).

107. *Gonzales* at 805.

108. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (striking down law that prohibited distribution of anonymous campaign literature); *see also* Talley v. California, 362 U.S. 60 (1960) (striking down a state law that forbade all anonymous leafletting).

because that material is harmful or obscene but merely because it is "directed at" minors! Thus, the content covered by COPPA 2.0 proposals could include not merely pornography, but communications about political nature, which deserved the highest degree of First Amendment protection.

2. Speech Rights of Site Operators

The necessary corollary of blocking adults from accessing certain content anonymously—and thereby deterring some users from accessing that content—is that COPPA 2.0, like COPA, would necessarily reduce the audience size of PI-collecting sites subject to age verification mandates. Furthermore, such mandates would encourage websites to self-censor themselves to avoid offering content they fear could be considered "directed at" adolescents because doing so might subject them to an age verification mandate—or to legal liability if they fail to implement age verification. The substantial cost of age verification could significantly impact, if not make impossible, the business models of many PI-collecting sites, which generally do not charge for content and rely instead on advertising revenues. The Third Circuit cited all of these burdens on the free speech rights of website operators in striking down COPA.[109]

3. Less Restrictive Alternatives to Regulation

The Third Circuit drew on the Supreme Court's 2004 decision striking down COPA on the grounds that "[b]locking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them."[110] Similarly, parental control software already empowers parents to restrict their kids' access to PI-collecting sites. (It's particularly easy for parents to restrict access to the leading social networking sites that seem to be driving so much of the push for COPPA 2.0, so that their kids.)

Thus, the free speech rights burdened COPPA 2.0 proposals are at least as important as those burdened by COPA, and blocking software already empowers parents to restrict their kids' access to PI-collecting sites, just as it allows parents to restrict access to pornography. Of course, if COPPA 2.0 laws were actually enacted and subject to legal challenge, the outcome of the case would depend largely on the level of constitutional scrutiny involved. COPPA 2.0 advocates might argue that, whatever the rights at stake, a lower level of constitutional scrutiny should apply because COPPA 2.0 does not target a special category of content. If true, this could mean that, although age verification mandates to restrict access to "harmful" material are unconstitutional, far more sweeping mandates restricting access to *non*-harmful information *could* be constitutional. Such inconsistency is indeed a perverse consequence of the fact that our First Amendment jurisprudence focuses not on the rights at stake, but on whether a regulation is "content-neutral" in deciding what level of scrutiny to apply—which, in

---

109. *See ACLU III*, 534 F.3d at 196-97 (citing *Gonzales* at 804). The Court held that websites "face significant costs to implement [COPA's age verification mandates] and will suffer the loss of legitimate visitors once they do so." *Id*. at 197.

110. *Id*. at 198 (quoting *ACLU v. Mukasey*, 534 F.3d 181, 198 (2008)).

turn, often determines the outcome of the case.[111] But in this case, COPPA 2.0 proposals likely *would* be subject to strict scrutiny to the extent that they are, like COPA, focused on a certain category of content: that "directed at" adolescents (rather than "harmful to minors").

Legislators who attempt to escape strict scrutiny by defining the scope of their bill (as in Illinois) not by its targeted audience but by reference to specific functional capabilities (in the definition of "social networking site")[112] will likely find that a court will see through such window-dressing: If they recognize that such bills are nonetheless aimed at a certain category of adolescent-oriented content, they will apply strict scrutiny anyway. But even under intermediate scrutiny, COPPA 2.0 proposals would be subject to serious attack.

B. First Amendment Rights of Adolescents

In addition, in COPPA 2.0 approaches, the government would restrict the ability of adolescents to access content, not because it could be harmful to them or because it is obscene, but merely because it is "directed to" them. While the First Amendment rights of minors may not be on par with those of adults, adolescents *do* have the right to access certain types of information and express themselves in certain ways.[113] The Supreme Court has held that "constitutional rights do not mature and come into being magically only when one attains the state-defined age of majority."[114] It remains unclear how an expanded COPPA model might interfere with the First Amendment rights of adolescents, but it is clear that privacy and speech rights would come into conflict under COPPA 2.0, as they do in other contexts.[115]

---

111. Ashutosh Avinash Bhagwat, *The Test that Ate Everything: Intermediate Scrutiny in First Amendment Jurisprudence*, 2007 U. Ill. Law. Rev. 783 (2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=887566.

112. *See supra* note 74.

113. *See* Theresa Chmara & Daniel Mach, *Minors' Rights to Receive Information Under the First Amendment*, Memorandum from Jenner & Block to the Freedom To Read Foundation, Feb. 2, 2004, www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/minorsrights.cfm (summarizing case law regarding minors' first amendment rights, especially in schools and in the context of mandates that public libraries filter Internet content); United States v. American Library Ass'n, 123 S. Ct. 2297 (2003), *available at* laws.findlaw.com/us/000/02-361.html (upholding the constitutionality of a filtering software system applicable to minors); *see generally*, Tinker v. Des Moines Ind. Comm. School Dist., 393 U.S. 503 (1969) (upholding students' rights to wear protest armbands and affirming that minors have speech rights) *available at* www.oyez.org/cases/1960-1969/1968/1968_21; *cf.* Morse v. Frederick, 551 U.S. 393 (2007), *available at* www.oyez.org/cases/2000-2009/2006/2006_06_278/ (holding that the First Amendment rights of students in school and at school-supervised events are not as broad as those of adults in other settings).

114. Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 74 (1976) (minors' right to abortion). *See also Bellotti v. Baird*, 443 U.S. 622, 635 n.13 (minors possess close to the "full capacity for individual choice which is the presupposition of First Amendment guarantees"); Catherine Ross, *An Emerging Right for Mature Minors to Receive Information*, 2 U. Pa. J. Const. L. 223 (1999); Lee Tien & Seth Schoen, Reply Comments of the Electronic Frontier Foundation filed in *Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming*, MB Docket No. 0926, Federal Communications Commission, May 18, 2009, http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520216901.

115. *See generally* Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 Fordham Intell. Prop. Media & Ent. L.J. 97 (2000), *available at*

For example, how might the parental-consent based model limit the ability of adolescents to obtain information about "safer sex" or how to deal with trauma, depression, family abuse, or addiction. Would an abusive father authorize a teen to visit a website about how to report child abuse? Would a parent of an adolescent struggling with their sexual identity let their kid participate in a self-help social networking page for gay and lesbian youth?[116] What rights are at play here and how do we reconcile them?

Maintaining the ability of kids to participate online interactions goes beyond content that most people would recognize as "serious"—from the perspective of both First Amendment values and the education of children. As a recent MacArthur Foundation study of the online youth Internet use concluded:

> Contrary to adult perceptions, while hanging out online, youth are picking up basic social and technological skills they need to fully participate in contemporary society. Erecting barriers to participation deprives teens of access to these forms of learning. Participation in the digital age means more than being able to access "serious" online information and culture.[117]

It was at least in part in recognition of such difficult First Amendment questions that Congress removed the requirement in the initial legislative draft of COPPA that would have required PI-based sites to "use reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17."[118]

---

http://law.fordham.edu/publications/articles/200flspub6588.pdf; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You,* 52 Stan. L. Rev. 1175 (2000), *available at* www.law.ucla.edu/volokh/privacy.htm.

116. "There are parents who, for a variety of reasons (political, cultural, or religious beliefs, ignorance of the facts, fear of being exposed as abusers, etc.), would deliberately prevent their teens from accessing social-network sites (SNS)." *ISTTF Final Report*, *supra* note 8, Appendix F, Statement of Connect Safely, at 262 (listing examples of unintended consequences of age verification mandates).

117. John D. and Catherine T. MacArthur Foundation, *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*, at 2 [hereinafter *MacArthur Study*] http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf.

118. This requirement was contained in the original bill, *supra note* 14 § 3(a)(2)(A)(iii), but was removed when that bill was reintroduced in its final form. In the interim, Congress held a hearing at which testimony was offered by, among others, Deirdre Mulligan of the Center for Democracy and Technology, which generally supported COPPA but argued for the very revisions that were ultimately made. In particular, Mulligan argued that:

> Under the bill each time a 15 year old signs-up to receive information through email his or her parent would be notified. For example if a 15 year old visits a site, whether a bookstore or a women's health clinic where material is made available for sale and requests information about purchasing a particular book or merely inquires about books on a particular subject (abuse, religion) using their email address the teenager's parent would be notified. This may chill older minors in pursuit of information.

Mulligan Testimony, *supra* note 15.

Even if parents have an absolute right to block their adolescents' access to such data, they can already exercise that right by applying strict controls on the computers in their home. COPPA 2.0 proposals go well beyond recognizing this right by setting the default to "parental consent required" for adolescents to access a wide range of content—meaning that parents must "opt-in" on behalf of their children before their children can participate in PI-collecting sites. This, in turn, burdens the ability of adolescents to communicate, because their parents might censor (rightly or wrongly) certain information, or simply fail to understand the technologies involved or to be actively engaged. But whatever the free speech rights of adolescents, if anyone should be interfering with those rights, it should be their parents—not the government.

Some parents may object that, however effective parental control software may be in the home, it does not allow parents to control what their kids' access *outside* the home. This argument is understandable on some level, but in the end, it amounts to a demand that roadblocks be put up everywhere for the sake of particularly sensitive parents at the expense of everyone else in society, including potentially huge numbers of adult users—and of online anonymity in general.

But Illinois's COPPA 2.0 proposal goes even further, not merely expanding COPPA to cover a particular variety of social networking sites,[119] but requiring that such sites "allow the parent or guardian of the minor unrestricted access to the profile webpage of the minor at all times."[120] Congress considered just such a parental access mandate in the initial draft of COPPA legislation back in 1998, but ultimately removed it from the final version of the legislation,[121] apparently because even some of COPPA's supporters worried, given the bill's initial application to the 13-16 age bracket, that "The establishment of a parental right to access all personal information about a teenager may intrude on older minors' privacy, rather than protect."[122]

C. Communication between Adolescents & Adults

Finally, COPPA 2.0 could infringe on the free speech rights of adults to communicate with adolescents online by driving PI-collecting sites to segregate users by age or to attempt to block access by adolescents. The vast majority of adult-minor interactions online are not of a harassing or predatory nature—indeed, they generally involve adults looking to help or assist minors in various ways. As the MacArthur Foundation study cited above concluded:

> In contexts of peer-based learning, adults … have an important role to play, though it is not the conventionally authoritative one. In friendship-driven practices, direct adult participation is often unwelcome, but in interest-driven groups we found a much stronger role for more experiences participants to play. Unlike instructors in

119. *See supra* note 74.

120. *SNWARA, supra* note 11, § 10(c).

121. The original COPPA bill required that parents have "access to the personal information of the child of that parent collected by that website," S. 2326**,** *supra* note 14, § 3(a)(2)(iv)(I), while the bill as passed instead requires only that parents be given "*a description of the specific types* of personal information collected from the child by that operator," 15 U.S.C. § 6502(b)(1)(B)(i) (emphasis added).

122. *See Mulligan Testimony*, *supra* note 118.

> formal educational settings, however, these adults are passionate hobbyists and creators, and youth see them as experienced peers, not as people who have authority over them. *These adults exert tremendous influence in setting communal norms and what educators might call "learning goals," though they do not have direct authority over newcomers.*[123]

A substantial portion of those interactions involve parents talking to their own kids, older and younger siblings communicating with one another, teachers and mentors talking to their students, or even co-workers of different ages communicating. Even when adult-minor communications involve complete strangers, there is typically a socially-beneficial purpose. Think of two people—one an adult and one a minor—debating politics on a discussion board, or creating a Wikipedia entry together. What about a presidential campaign website that involves millions of volunteers of all ages communicating and collaborating to a common purpose? There are countless other examples. How would such interactions be affected by COPPA 2.0? Restricting such interactions would raise profound First Amendment concerns about freedom of speech as well as of association.

In any First Amendment analysis, a court must consider not only the free speech rights at stake and the availability of less restrictive alternatives to regulation, but the governmental interest being advanced. Again, neither COPPA nor the COPPA 2.0 proposals discussed herein (in New Jersey and Illinois) requires exclusion of older users from a website, nor directly governs the sharing of personal information among users (where that sharing does not also constitute collection by the site itself). But separation of adolescents from adults is likely to be an indirect effect of COPPA 2.0 requirements—as COPPA 2.0 advocates probably realize—because, once PI-collecting sites are required to age-verify users, they will face reputational, political and potentially legal pressure to make interactions between adolescents and children more difficult in the name of "child safety." More subtly, if PI-collecting site operators have an incentive to avoid being considered "directed at" adolescents, they will also have an incentive to discourage adolescent participation on their site—which achieves a similar result.

Here, one must further ask if attempting to quarantine children from adults (however indirectly) actually advances, on net, a strong governmental interest in child protection. Such a quarantine is unlikely to stop adults with truly nefarious intentions from communicating with minors, as systems designed to exclude participation by adults in a "kids-only" or "adolescents-only" area can be easily circumvented. Given the lack of strong identity records for minors, it's much easier for an adult to pretend to be a minor than vice versa. The effect of age stratification on truly bad actors is likely to be marginal at best—or harmful at worst: Building walls around adolescents through age-verification might actually make it *easier* for predators to target teens, since a predator who gains access to a supposedly teen-only site will be *less* likely to be exposed as a predator by targeting an adult they think is a teen. So for the sake of marginal (if any) gains in child protection, would we not be excluding *beneficial* interaction between adults and minors?

---

123. *MacArthur Study*, *supra* note 117, at 39 (emphasis added).

To hear some of the advocates of COPPA 2.0 talk about how teens currently behave online, one might think that online environments in which adolescents were left to their own devices—imagine a "Teen MySpace" for the 13-17 crowd, walled off from the rest of MySpace—would be far worse, perhaps an online version of *Lord of the Flies*. These concerns are clearly exaggerated: The critics frequently complain about "the way kids talk to each other these days" while looking at their own past adolescent banter with rose-colored lenses. What *is* clear is that adolescents (and young adults) behave *better* in online environments where adults are present, too. Perhaps the best demonstration of this fact has been the uproar from adolescents and young adults that has accompanied Facebook's explosive growth in popularity among older users in recent months.[124] Many kids hate the idea of adults joining Facebook precisely because the presence of adults encourages kids to "self-regulate" by exercising better judgment and following better netiquette.[125]

Anne Collier, founder and executive director of the child safety advocacy organization Net Family News, Inc. and editor of NetFamilyNews.org and ConnectSafely.org, suggests that the push for "segregation" by age (*e.g.*, creating a teen-only version of Second Life) for safety's sake is "losing steam" because:

> it's a response to the predator panic teens and parents have been subjected to in U.S. society, not to the realities of youth on the social Web. What nearly a decade of peer-reviewed academic research shows is that peer-to-peer behavior is the online risk that affects many more youth, the vast majority of online kids who are not already at-risk youth offline. Segregating teens from adults online doesn't address harassment, defamation, imposter profiles, cyberbullying, *etc*. It may help keep online predators away from kids (even though online predation, or abuse resulting from online communication, constitutes only 1% of overall child sexual exploitation…), which is a great outcome, but it's not enough unless all that parents are worried about is predators.[126]

---

124. Justin Smith, *Number of US Facebook Users Over 35 Nearly Doubles in Last 60 Days*, Inside Facebook Blog Mar. 25, 2009, www.insidefacebook.com/2009/03/25/number-of-us-facebook-users-over-35-nearly-doubles-in-last-60-days/.

125. *See, e.g.*, Lori Aratani, *When Mom or Dad Asks To Be a Facebook "'Friend,"* The Washington Post, Mar. 9, 2008, www.washingtonpost.com/wp-dyn/content/article/2008/03/08/AR2008030801034.html. "'I do not know if this has happened to anybody, but this morning I log on to Facebook and I have a new friend request!' wrote 19-year-old Mike Yeamans, a sophomore at James Madison University, on one of several 'No Parents on Facebook' groups that have popped up on the site. 'I am excited to make a new friend so I click on the link. I could not believe what I saw. My father! This is an outrage!'" *Id*.

126. Anne Collier, *Where Will OnlineTeens Go Next?*, May 1, 2009, www.netfamilynews.org/2009/05/where-will-online-teens-go-next.html (internal citations omitted). For evidence of at-risk youth, Collier sites the *ISTTF Final Report*, *supra* note 8. Regarding the percentage of all child sexual exploitation that results from online communication, she cites Janis Wolak, David Finkelhor & Kimberly Mitchell, Crimes Against Children Research Center, *Trends in Arrests of Online Predators*, 2009) www.unh.edu/ccrc/pdf/CV194.pdf; *see also*, Anne Collier, *Major Update on Net predators: CACRC study*, March 31, 2009, www.netfamilynews.org/2009/03/major-update-on-net-predators-mostly.html (summarizing study).

Collier discusses the particularly acute problem of "actual or perceived sexual orientation and gender expression," which the *Salt Lake Tribune* has noted are "two of the top three reasons secondary school students said their peers were most often bullied at school."[127] This kind of harassment recently attracted widespread public attention after two 11-year-old boys committed suicide after experiencing anti-gay harassment and bullying at school.[128] Nationwide, "Lesbian, gay, bisexual, transgender and questioning youth are up to four times more likely to attempt suicide than their heterosexual peers."[129] This child safety risk is painfully real, with anti-gay harassment being only its most obvious form. But "segregating" teens from adults seems likely to aggravate this problem by removing adults from the mix as a potential source of discipline.

Of course, adults play a critical role in disciplining interaction among the 0-12 age bracket, but not as direct participants in on-site interaction. Again, how many adults actually want to use Club Penguin? Instead, parents can supervise what their kids do online through parental control software. Parents could, of course, use that same software to monitor what their adolescent kids do, too. But as kids get older, most parents realize that the training wheels have to come off at some point. Few parents will want to spy on their 17-year old until the day before the kid starts college (or enlists in the military or gets married). But most parents probably *would* prefer that, if their kids are interacting in an online environment, they think twice about what they do and say online. It is by no means clear that restricting online interaction between teens and adults will serve that end.

VII. The Commerce Clause Implications of State-Level COPPA 2.0

State-based efforts to expand COPPA or to impose other forms of age/identity verification raise additional constitutional concerns: State-level efforts by state government or state AGs to push through an expansion of COPPA would likely violate the Commerce Clause of the U.S. Constitution.

For simplicity, the preceding discussion did not consider how PI-collecting sites would respond to COPPA obligations imposed in one U.S. state but not others. Sites might default to the "lowest common denominator" of whatever would be acceptable in the most restrictive states—especially if those states has populations as large as Illinois or New Jersey. But websites could also attempt to configure their services to function differently depending on what state the user is in. Thus, age verification mandates might also require location mandates (again, perversely requiring the collection of *more* information in the name of protecting adolescents' privacy). If a site relied only on location information provided by the user, adolescents would quickly learn to lie about what state they live in just as children have learned to lie about how

---

127. Anne Collier, *Anti-Gay Bullying Most Pervasive*, April 29, 2009, www.netfamilynews.org/2009/04/anti-gay-bullying-most-pervasive.html (quoting Charles Robbins & Eliza Byard, *Gay Suicide: Addressing Harassment in Schools*, Salt Lake Tribune, April 24, 2009, www.sltrib.com/opinion/ci_12220931 [hereinafter *Gay suicide*]).

128. *Gay suicide*, *supra* note 127.

129. *Id*.

old they are to avoid triggering COPPA's "actual knowledge" requirement. Alternatively, websites could attempt to determine a user's location automatically based on their IP address, but such "IP geocoding" is not always accurate and can be subverted by use of a proxy.

This technical discussion should help to illustrate why state-level COPPA 2.0 proposals would burden communication over the Internet, a uniquely "interstate" medium whose architecture makes it difficult, if not impossible, to isolate the effects of state regulation on residents of that state. There is a long string of "Dormant Commerce Clause" cases that have consistently struck down state laws attempting to regulate commerce (or speech) that originates or takes place outside the state's borders.[130] If it is not possible for a state government to isolate the effects of its regulatory actions to merely those PI-collecting site operators or users living within its jurisdiction, federal courts will block such measures. Consequently, the extraterritorial impact of state-based COPPA expansion would likely result in an immediate constitutional challenge and such regulation would almost certainly be overturned.

It is also possible that COPPA 2.0 proposals may already be pre-empted by COPPA because, although COPPA authorizes state attorneys general to bring enforcement actions under certain circumstances,[131] COPPA bars states from enacting any laws "inconsistent" with COPPA.[132]

VIII. Summary of Implementational Challenges Regarding COPPA Expansion

Even if one somehow overcame the many policy and constitutional arguments against COPPA 2.0, there would remain a slew of difficult, if not impossible, challenges to overcome in implementing such a system. Most critically, the threshold practical question remains the same as it does for most other forms of online identity verification: *How do we verify the parent-child relationship when someone asserts they are the parent or guardian*? But there are many other questions regarding how well COPPA would "scale up" that must be considered:

1. **Verification Mechanisms**. What sort of mechanisms will need to be put in place to guarantee that the parent or guardian is who they claim to be (for both initial enrollment and subsequent visit authentication)? Sign-and-fax forms can be easily forged, so credit cards (and perhaps mandatory user fees) will likely become the default solution. A third method, follow-up phone calls, just doesn't seem practical. But might lawmakers demand a mix of all of the above?
2. **Obtaining Consent**. Regardless, how burdensome will those mandates be on parents or guardians? As Parry Aftab has noted, "The more difficult we make the consent mechanism, the fewer parents we will get to consent."[133]

---

130. *See* Adam Thierer, *The Delicate Balance: Federalism, Interstate Commerce, and Economic Freedom in the Technological Age* at 58-61 (The Heritage Foundation, 1999).

131. 15 U.S.C. § 6504.

132. "No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section." 15 U.S.C. § 6502(d).

133. *Aftab Comments*, *supra* note 59, at 5.

3. **Costs to Business**. How burdensome will those mandates be for PI-collecting site operators? What kind of compliance costs or legal penalties are we talking about?
4. **Costs to Users**. Will those costs be passed on to users as fees beyond the nominal transactions required to achieve verification via credit cards? (Since most PI-collecting sites websites and almost all social networking sites are free-of-charge today, that's not going to be a very popular mandate!)[134]
5. **Disparate Socio-economic Effects**. How would increased fees or credit card mandates impact low-income families and youth, especially those without credit cards?
6. **Industry Consolidation**. If compliance costs—in the form of additional staff, insurance and litigation expenses—explode for website operators, will this cause the kind of industry consolidation that seems to have occurred with child-oriented websites since COPPA's adoption? Would the increased hassle of accessing new sites lead to consolidation by reducing adoption rates by users? How would online innovation and creative expression suffer as a result of such consolidation?
7. **Increased Privacy Risks**. Who would collect the massive databases of information created by such a mandate? Who has access to all that new data? What might government use it for if they get their hands on it?
8. **Offshore Sites**. Could this new regime be applied effectively to offshore sites? Or, will kids flock to offshore sites as a result of such mandates on domestic sites? If some do, how will we stop them?
9. **Credential Transferring**. Even if the parental permission verification process worked during initial enrollment, how would it work in the "subsequent visit" stage? Once minors are given credentials or digital tokens, how do we prevent them from sharing or selling their credentials? In particular, how do we prevent older siblings from sharing their credentials with younger siblings? What would be the penalty for them doing so? What about older minors with independent access to credit cards?
10. **Law Enforcement Priorities**. How many law enforcement or regulatory agencies will be tasked with administering this regulatory regime? Might this be diverting resources from better priorities, such as serious law enforcement efforts and online safety educational programs?

IX. Conclusion

The future of age verification battles—at least on the social networking front—will likely be fundamentally tied up with COPPA and the question of how well parental consent-based forms of age verification might work on a scale larger than COPPA's very limited scale. It is unlikely, however, that such a framework could be easily applied on "Internet scale." There is a world of difference between a site like Disney's Club Penguin, for example, and sites like MySpace or

134. Aftab also notes that "Parents do not trust a site to use their credit card to verify their consent. They barely trust online credit card use when they want to buy something." *Id.*

Facebook. This ultimately reflects the uniquely insular nature of the under-13 age bracket and the lack of any clear line between adolescent-oriented and "general audience" content.

Moreover, as social networking capabilities become increasingly ubiquitous, integrated into every site and service—from Change.gov[135] to the San Francisco Chronicle (sfgate.com) to CNN.com, from Microsoft's Xbox Live service to Linden Labs' Second Life—the costs and hassles of compliance with COPPA 2.0 age verification mandates will increase dramatically. Are parents really going to be forced to authenticate themselves and then their kids for every website their kids want to participate in that requires so much as an e-mail address? That mandate seems unnecessary and unworkable. Are other adults going to have to prove they're not adolescents? By creating such a requirement, COPPA 2.0 would also constitute a functional convergence of COPPA with COPA—a law the courts have rejected as inconsistent with America's tradition of anonymous speech, something central to our evolution as a democracy, pre-dating even the First Amendment that protects it from government interference.

Finally, the irony of COPPA 2.0 proposals is that lawmakers would be applying a law that was meant to protect the privacy and personal information of children to gather a great deal *more* information about them, their parents, and many other adults! These privacy implications should make us think twice about trying to expand COPPA beyond its primary purpose to encourage parental involvement in what kids do online. Even those who support COPPA in its current form should recognize that there are better ways to protect adolescents online.[136]

135. Like many social networking sites, Change.gov allows users to comment on news items the IntenseDebate comment platform, which allows users to create profiles, upload profile photos, *etc*.

136. *See Parental Controls and Online Child Protection: A Survey of Tools and Methods*, *supra* note 17.

Related PFF Publications

- *Targeted Online Advertising: What's the Harm & Where Are We Heading?*, Berin Szoka & Adam Thierer, Progress on Point 16.2, April 2009.
- *Parental Controls & Online Child Protection: A Survey of Tools and Methods*, Adam Thierer, Special Report, Version 3.1, Fall 2008.
- *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, Adam Thierer, Progress on Point 14.5, March 21, 2007.
- *Social Networking Websites & Child Protection: Toward a Rational Dialogue*, Adam Thierer, Progress Snapshot 2.17, June 2006.
- *Age Verification for Social Networking Sites: Is It Possible? And Desirable?*, Adam Thierer, Progress on Point 14.8, March 23, 2007.
- *Is MySpace the Government's Space?*, Adam Thierer, Progress Snapshot 2.16, June 2006.
- *Rep. Bean's 'SAFER Net Act': An Education-Based Approach to Online Child Safety*, Adam Thierer, Progress on Point 14.3, Feb. 22, 2007.
- *Online Advertising & User Privacy: Principles to Guide the Debate*, Berin Szoka & Adam Thierer, Progress Snapshot 4.19, Sept. 2008.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
202-289-8928 ■ mail@pff.org ■ www.pff.org

THE PROGRESS & FREEDOM FOUNDATION

Written Testimony of
Berin Szoka
Senior Fellow, The Progress & Freedom Foundation
& Director of PFF's Center for Internet Freedom
www.pff.org

Hearing on
"An Examination of Children's Privacy: New Technologies & the Children's Online Privacy Protection Act"

Before the
Subcommittee on Consumer Protection
Committee on Commerce, Science & Transportation
U.S. Senate

April 29, 2010

Mr. Chairman and Committee members, thank you for inviting me here today. My name is Berin Szoka.[1] I'm a Senior Fellow at The Progress & Freedom Foundation (PFF). PFF is a market-oriented think tank and 501(c)(3) non-profit founded in 1993 that studies the digital revolution and its implications for public policy. PFF's mission is to educate policymakers, opinion leaders, and the public about issues associated with technological change, based on a philosophy of limited government, free markets, and individual sovereignty.

I commend this Committee for studying the Children's Online Privacy Protection Act or COPPA, and the FTC for its upcoming COPPA Review and Roundtable.[2] My colleague Adam Thierer, PFF's President, has been actively engaged in debates about online child safety and privacy since joining PFF in 2005, and is the author of *Parental Controls & Online Child Protection: Survey of Tools & Methods,* a regularly updated compendium now in its fourth edition and available for free online.[3] The constant theme in PFF's work in this area has been to emphasize the tools and methods available to parents to control their children's use of media, including the Internet and to the central role played by education efforts in helping both parents and children make smarter choices. We also highlight enforcement of existing laws as an additional "less restrictive" alternative to new regulation, and attempt to highlight the trade-offs involved in imposing new regulation of online communications.

---

1 The views expressed here are his own, and not necessarily the views of the PFF board, other fellows or staff.

2 Federal Trade Commission, *Request for Public Comment on the FTC's Implementation of the Children's Online Privacy Protection Rule*, April 5, 2010, http://www.ftc.gov/os/2010/03/100324coppa.pdf; *see also* COPPA Rule Review Roundtable, http://www.ftc.gov/bcp/workshops/coppa/index.shtml.

3 Adam Thierer, *Parental Controls & Online Child Protection: Survey of Tools & Methods*, Version 4.0, Fall 2008, www.pff.org/parentalcontrols/index.html.

In May 2009, Adam and I published a 35-page paper entitled *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, providing an overview of COPPA, how it works, its costs and benefits, and explaining the dangers inherent in several then-pending efforts to expand COPPA by expanding the law to cover adolescents or all social networking sites.[4] We identified a number of legal, technical, and other practical problems with such proposals in that they would:

- Burden the free speech rights of adults by imposing age verification mandates on many sites used by adults, thus restricting anonymous speech and essentially converging—in terms of practical consequences—with the unconstitutional Children's Online Protection Act (COPA),[5] another 1998 law sometimes confused with COPPA;
- Burden the free speech rights of adolescents to speak freely on—or gather information from—legal and socially beneficial websites;
- Hamper routine and socially beneficial communication between adolescents and adults;
- Reduce, rather than enhance, the privacy of adolescents, parents and other adults because of the massive volume of personal information that would have to be collected about users for authentication purposes (likely including credit card data);
- Would likely be the subject of massive fraud or evasion since it is not always possible to definitively verify the parent-child relationship, or because the system could be "gamed" in other ways by determined adolescents;
- Do nothing to prevent offshore sites and services from operating outside these rules;
- Present major practical challenges for law enforcement officials in the face of such evasion by both domestic users and offshore sites;
- Could destroy opportunities for new or smaller website operators to break into the market and offer competing services and innovations, thus contributing to consolidation of online content and services by erecting barriers to entry; and
- Violate the Commerce Clause of the U.S. Constitution if enacted by states, since Internet activity clearly represents interstate commerce that states have no authority to regulate.

This testimony summarizes the key aspects of that paper, but also provides additional context on subsequent developments and related issues. Subsequently, I filed written testimony with the Maine Legislature regarding proposals in Maine, including a law enacted over the summer but never enforced by the state attorney general, to apply the COPPA framework to the collection of health-related information from adolescents.[6] We also look forward filing comments in the FTC's upcoming COPPA Review.

---

[4] Berin Szoka & Adam Thierer, *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, Progress on Point 16.11, May 2009, http://pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-verification.pdf.

[5] 47 U.S.C. § 231. While COPPA governs sites "directed at" children, COPA would have required age verification for content deemed "harmful to minors." COPA has been struck down on First Amendment grounds.

[6] Berin Szoka, *Written to Maine Legislature on Act to Protect Minors from Pharmaceutical Marketing Practices, LD 1677*, March 4, 2010, www.pff.org/issues-pubs/filings/2010/2010-03-04-Maine_Law_Testimony.pdf.

COPPA can best be summarized as follows: For an "Internet Jr." of sites "directed at" children under 13, COPPA requires sites either to age-verify all users or limit functionality to prevent children from making personal information "publicly available"—including the sharing of user-generated content. COPPA imposes the same requirement on general audience sites when they have actual knowledge a user is under 13.

The Costs of COPPA

Because of this forced separation and the costs of age verification, COPPA may well have unintentionally limited choice and competition by driving increased consolidation in the marketplace for child-oriented sites and services online and discouraging new entry by smaller "mom-and-pop" sites that could cater to children. As early as 2001, even some Congressmen recognized this "unintended consequence" of COPPA in Congressional hearings on privacy.[7] There are significant costs associated with the verifiable parental consent methods used to comply with COPPA. Of course, it could be the case that there are other reasons that there are relatively few sites catering exclusively to children. But this is a question worth considering, and the FTC deserves credit for beginning its COPPA review with this question.[8] As noted by Parry Aftab, Executive Director of the children's advocacy group Wired Safety, "COPPA wasn't responsible for the demise of these sites, but when combined with the other factors [it] tipped the balance."[9] She concludes, appropriately:

> It is crucial that at this tentative stage for the kids Internet industry we don't do anything to make its survival more difficult. We should be looking at easy to encourage safer communities for preteens and innovations to help create fun, entertaining and educational content for kids online.[10]

The Success of COPPA

On the other hand, COPPA has been reasonably successful in fulfilling Congress's original goals, as expressed by the law's Congressional sponsors:

---

[7] Rep. Billy Tauzin (R-LA) noted that COPPA "has now forced companies to discontinue a number of products targeted toward children" and asked "If we end up forcing private companies and nonprofits to eliminate beneficial products such as crime prevention material, have we done a good thing? If teen-friendly sites, those that totally respect the privacy of the users stop offering e-mail services to children, is that a good thing? *An Examination of Existing Federal Statutes Addressing Information Privacy: Hearing of the House Committee On Energy and Commerce*, 107th Cong. 6 (April 3, 2001) (statement of Rep. Tauzin.), *available at* http://republicans.energycommerce.house.gov/107/action/107-22.pdf.

[8] Federal Trade Commission, *Request for Public Comment on the FTC's Implementation of the Children's Online Privacy Protection Rule*, at 2 April 5, 2010, http://www.ftc.gov/os/2010/03/100324coppa.pdf.

[9] *Comments of Parry Aftab, Request for Public Comment on the Implementation of COPPA and COPPA Rule's Sliding Scale Mechanism for Obtaining Verifiable Parental Consent Before Collecting Personal Information from Children* at 3, June 27, 2005, www.ftc.gov/os/comments/COPPArulereview/516296-00021.pdf

[10] *Id.*

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[11]

Thus, as its name implies, COPPA is first and foremost about protecting the privacy of children. COPPA's primary means for achieving this goal is enhancing parental involvement or, as the FTC has put it, "provid[ing] parents with a set of effective tools… for becoming involved in and overseeing their children's interactions online."[12] However admirable, "protect[ing] the safety of children" is merely an *indirect* goal of COPPA—something to be achieved through the means of enhancing parental involvement (COPPA's *direct* goal). The FTC declares that COPPA "has provided a workable system to help protect the online safety and privacy of the Internet's youngest visitors."[13]

Indeed, COPPA may succeed in achieving its original purpose of enhancing parental involvement, but strict age verification mandates intended to go beyond COPPA will ultimately fail because kids will simply lie to circumvent age verification requirements. As Microsoft researcher danah boyd has put it, "COPPA did not stop most children from creating accounts, but it did teach children and their parents an important lesson: Lying is the path to access."[14] Even though "there is no perfect solution" and it is not possible to completely "stop a child from lying and putting themselves at risk," Denise Tayloe of Privo, one of the four FTC-approved providers of COPPA safe harbor age verification services, believes that COPPA "provides a platform to educate parents and kids about privacy."[15]

Especially given this practical limitation and whatever the trade-offs involved in COPPA, I'm here today to caution against expanding COPPA beyond its original, limited purpose. COPPA's unique value lies in its flexibility, subtlety, and intentional narrowness.

COPPA is Flexible Enough to Cover a Rapidly Changing Landscape

COPPA is flexible because it potentially applies to the entire Internet regardless of the access device used—including services scarcely imaginable in 1998. Specifically, COPPA applies to any "operator," which the statute defines to mean:

---

11 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

12 Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* at 28, Feb. 2007, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

13 *Id*.

14 danah michele boyd, *Taken Out of Context American Teen Sociality in Networked Publics*, at 151 Fall 2008, www.danah.org/papers/TakenOutOfContext.pdf.

15. E-mail from Denise Tayloe to Adam Thierer (Mar. 15, 2007) (copy on file with author).

> any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce.[16]

COPPA defines the key term "Internet" broadly to mean:

> collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/ Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.[17]

In interpreting its COPPA Rule, the FTC has said:

> The Rule's Statement of Basis and Purpose makes clear that the term Internet is intended to apply to broadband networks, as well as to intranets maintained by online services that either are accessible via the Internet, or that have gateways to the Internet.[18]

Because nearly all communications platforms have converged on the "Internet," thus defined, COPPA would reach a wide variety of services and media not commonly thought of as belonging to the "Internet." For example, if a video game console is networked through the Internet to allow users to play games with each other, COPPA would apply to potential sharing of personal information. To this extent, the FTC ought not need new statutory authority from Congress.

COPPA's Subtlety Lies in its Narrowness

COPPA is subtle because it requires "verifiable parental consent" not only if site and service operators gather personal information from kids for their own use, but also if sites enable children to make personal information "publicly available" online. Even more subtle is COPPA's creative solution to the thorny problem of age verification. Unlike the similarly-named Child Online Protection Act of 1998 (COPA, pronounced "*koh-pah*" instead of "*kah-pah*"),[19] COPPA only requires age verification of users on sites clearly directed at children, whereas COPA required it for any site offering content deemed "harmful to minors."

---

16 15 U.S.C. § 6501(2).

17 15 U.S.C. § 6501(6).

18 Federal Trade Commission, *Frequently Asked Questions about the Children's Online Privacy Protection Rule*, Question 6 ("What types of online transmissions does COPPA apply to?"), www.ftc.gov/privacy/coppafaqs.shtm

19 47 U.S.C. § 231.

Efforts to Expand COPPA Raise Serious First Amendment Concerns

Back in 1998, Congress wisely chose not to apply COPPA to adolescents. Unfortunately, recent efforts to expand COPPA have put online privacy, child safety, free speech and anonymity on a collision course. Several states have proposed what we at PFF have called "COPPA 2.0" laws, extending COPPA to adolescents up to 17 or 18. But once the age threshold rises above 13, it becomes increasingly difficult to distinguish sites "directed at" children below the threshold from general audience sites. With this seemingly small change, COPPA would essentially converge with COPA: COPPA would extend beyond a discrete "Internet, Jr." to require age verification for sites used by many adults—and, indeed, other states have proposed simply extending COPPA to all social networking sites. But requiring adults and even older teens to prove their age by identifying themselves constitutes a prior restraint on anonymous or pseudonymous communication. This raises the same First Amendment concerns that caused the courts to strike down COPA.

After a decade-long court battle over COPA's constitutionality, the U.S. Supreme Court in January 2009 rejected the government's latest request to revive the law, meaning it is likely dead.[20] Three of the key reasons the courts struck down COPA would also apply to COPPA 2.0 proposals:

- **Anonymous Speech Rights of Adults**. COPA burdened the speech rights of adults to access information subject to age verification requirements, both by making speech more difficult and by stigmatizing it. In 2003, the Third Circuit noted that age verification requirements "will likely deter many adults from accessing restricted content, because many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial."[21] The Supreme Court has recognized the vital importance of anonymous speech in the context of traditional publication.[22] By imposing broad age verification requirements, COPPA 2.0 would restrict the rights of adults to send and receive information anonymously just as COPA did. If anything, the speech burdened by COPPA 2.0 deserves *more* protection, not less, than the speech burdened by COPA: Where COPA merely burdened access to content deemed "harmful to minors" (*viz*., pornography), COPPA 2.0 would burden access to material by adults as well as minors not because that material is harmful or obscene but merely because it is "directed at" minors! Thus, the content covered by COPPA 2.0 proposals could include not merely pornography, but communications about political nature, which deserved the highest degree of First Amendment protection.

---

[20] *See* Adam Thierer, The Progress & Freedom Foundation, *Closing the Book on COPA*, PFF Blog, Jan. 21, 2009, http://blog.pff.org/archives/2009/01/closing_the_boo.html. *See also* Alex Harris, *Child Online Protection Act Still Unconstitutional*, http://cyberlaw.stanford.edu/packet/200811/child-online-protection-act-still-unconstitutional.

[21] American Civil Liberties Union v. Ashcroft, 322 F.3d 240, 259 (3d Cir. 2003).

[22] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (striking down law that prohibited distribution of anonymous campaign literature); *see also* Talley v. California, 362 U.S. 60 (1960) (striking down a state law that forbade all anonymous leafletting).

- **Speech Rights of Site Operators**. The necessary corollary of blocking adults from accessing certain content anonymously—and thereby deterring some users from accessing that content—is that COPPA 2.0 proposals would, like COPA, necessarily reduce the audience size of websites subject to age verification mandates. Furthermore, such mandates would encourage websites to self-censor themselves to avoid offering content they fear could be considered "directed at" adolescents because doing so might subject them to an age verification mandate—or to legal liability if they fail to implement age verification. The substantial cost of age verification could significantly impact, if not make impossible, sites that allow sharing of personal information, including user-generated content, because such sites generally do not charge for content and rely instead on advertising revenues. The Third Circuit cited all of these burdens on the free speech rights of website operators in striking down COPA.[23]
- **Less Restrictive Alternatives to Regulation**. The Third Circuit drew on the Supreme Court's 2004 decision striking down COPA on the grounds that "[b]locking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them."[24] Similarly, parental control software already empowers parents to restrict their kids' access to sites that "collect" personal information. It's particularly easy for parents to restrict access to the leading social networking sites that seem to be driving so much of the push for COPPA 2.0.

COPPA Expansion Would Undermine Privacy

Ironically, broad age verification mandates would *reduce* online privacy by requiring *more* information to be collected from both adolescents and adults, including credit card information, in order to verify age and the parent/child relationship (in the admittedly imperfect fashions prescribed by COPPA's "Sliding Scale"). While COPPA's safe harbor administrators play a valuable role in administering self-regulation under COPPA,[25] government shouldn't put them in the awkward position of becoming repositories for huge troves of personal information in the name of protecting privacy.

COPPA Expansion Would Not Enhance Child Safety

Some have argued that age verification mandates could protect children by allowing sites to create "safe spaces" that exclude predators. Unfortunately, the reality is that the technology for reliable age verification simply doesn't exist.

---

[23] *See ACLU III*, 534 F.3d at 196-97 (citing ACLU v. Gonzales, 478 F. Supp. 2d 775, 804). The Court held that websites "face significant costs to implement [COPA's age verification mandates] and will suffer the loss of legitimate visitors once they do so." *Id*. at 197.

[24] *Id*. at 198 (quoting *ACLU v. Mukasey*, 534 F.3d 181, 198 (2008)).

[25] The four safe harbor programs are administered by the Children's Advertising Review Unit of the Council of Better Business Bureaus (CARU); the Entertainment Software Rating Board (ESRB); TRUSTe; and Privo. *See* Federal Trade Commission, *Safe Harbor Program*, www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html.

Federal courts have found that there is "no evidence of age verification services or products available on the market to owners of Web sites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor."[26] Few public databases exist that could be referenced to conduct such verifications for minors, and most parents do not want the few records that *do* exist about their children (*e.g.*, birth certificates, Social Security numbers, school records) to become more easily accessible.[27] Indeed, concerns about those records being compromised or falling into the wrong hands have led to legal restrictions on their accessibility.[28] Even the FTC has made clear that it doesn't consider COPPA's "sliding scale" of verifiable parental consent methods—use of a credit card, print-and-fax forms, follow-up phone calls and e-mails, and using encryption certificates[29]—as equivalent to strict age verification.[30]

Fears of Advertising Should Not Drive COPPA Expansion

COPPA expansion could also undermine the viability of many online sites and services. Some consider marketers the "real predators"—even though advertising is the great "Hidden Benefactor"[31] that funds the overwhelming majority of "free" Internet content and services. COPPA already applies to the collection of information that could potentially allow the contacting of a child under 13. The Network Advertising Initiative already requires verifiable parental consent for behavioral advertising to children under 13. But if COPPA were expanded to require general audience sites funded by tailored advertising to age-verify all users, it would devolve into the unconstitutional approach found in COPA. Importantly, COPPA expansion would also raise costs for smaller or new sites and services geared toward minors. This could discourage new innovation, limit choice, and raise prices for consumers.[32]

---

[26] *Gonzales*, 478 F. Supp. 2d at 806.

[27] *See* Adam Thierer, The Progress & Freedom Foundation, *Age Verification Debate Continues; Schools Now at Center of Discussion*, PFF Blog, Sept. 25, 2008, http://blog.pff.org/archives/2008/09/age_verificatio_1.html.

[28] Various laws and regulations have been implemented that shield such records from public use, including various state statutes and the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[29] 16 C.F.R. § 312.5(b)(2).

[30] In a February 2007 report to Congress about the status of the law and its enforcement, the FTC said that no changes to COPPA were then necessary because the law had "been effective in helping to protect the privacy and safety of young children online." Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* at 1, Feb. 2007, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf. In discussing the effectiveness of the parental consent verification methods authorized in the FTC's sliding scale approach, however, the agency acknowledged that "none of these mechanisms is foolproof." *Id*. at 13. The FTC attempts to distinguish these parental consent verification methods from other kinds of age verification tools in noting that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms." *Id*. at 12.

[31] Adam Thierer & Berin Szoka, *The Hidden Benefactor: How Advertising Informs, Educates & Benefits Consumers*, Progress on Point 6.5, Feb. 2010, www.pff.org/issues-pubs/ps/2010/pdf/ps6.5-the-hidden-benefactor.pdf.

[32] In 2005, the FTC has cited an estimate of $45/child as the cost of obtaining verifiable parental consent for child-oriented sites to comply with COPPA. *See Comments of Parry Aftab, Request for Public Comment on the*

Ultimately, concerns about tailored advertising may be less about privacy than about what advertising scholar Jack Calfee has dubbed the "Fear of Persuasion"—the idea that advertising is inherently manipulative and only grows more so with increased relevance. But as Calfee notes, "by the age 10 or so, children develop a full understanding of the purpose of advertising and equally important, an active suspicion of what advertisers say."[33] If government has a role to play in addressing concerns about tailored marketing, it lies in educating kids about advertising to help them become smarter consumers. Last week, the FTC launched just such an education campaign with its AdMongo tutorial website (www.admongo.gov).[34] The FTC excels in consumer education, and should be encouraged in these efforts as a less restrictive alternative to regulation. Other excellent examples of FTC education efforts include:

- On Guard Online (online security, fraud avoidance & privacy tips) (OnGuardOnline.gov);
- *NetCetera: Chatting With Kids About Being Online* (www.onguardonline.gov/topics/net-cetera.aspx); and
- *You Are Here: Where Kids Learn to be Smarter Consumers* (ftc.gov/youarehere/).

Opening the Door to COPPA Expansion through FTC Overhaul via Financial Reform

Finally, financial reform legislation recently passed by the House would give the FTC sweeping new rulemaking powers, and could allow the FTC to unilaterally change COPPA, including its age range. Specifically, H.R. 4173 would give the FTC normal rulemaking authority under the Administrative Procedures Act, replacing the special rulemaking procedures crafted by Congress with the 1975 Magnuson-Moss Act, and strengthened through additional procedural safeguards in 1980, to ensure that the agency did not rush into preemptive regulation without carefully weighing the costs and benefits of government intervention.[35]

Such decisions should be made by Congress, not the FTC. If Congress wants to help the FTC implement COPPA, it should consider additional funding for education and enforcement. These, in conjunction with empowerment of parents and kids to manage their own privacy and other online preferences, offer a better approach to addressing concerns about online child privacy and safety than increased regulation.

Thank you again for inviting me to testify.

Implementation of COPPA and COPPA Rule's Sliding Scale Mechanism for Obtaining Verifiable Parental Consent Before Collecting Personal Information from Children at 2, June 27, 2005, www.ftc.gov/os/comments/COPPArulereview/516296-00021.pdf.

[33] Jack Calfee, American Enterprise Institute, *Fear of Persuasion: A New Perspective on Advertising and Regulation,* 59 (1997).

[34] *Federal Trade Commission to Launch Advertising Literacy Campaign National Program Gives 'Tweens' Ages 8 to 12 Skills to Recognize, Understand Advertising*, April 26, 2010, www.ftc.gov/opa/2010/04/admongo.shtm.

[35] *See generally*, Berin Szoka, *How Financial Overhaul Could Put the FTC on Steroids & Transform Internet Regulation Overnight*, Progress Snapshot 6.7, March 2010, www.pff.org/issues-pubs/ps/2010/pdf/ps6.7-FTC_on_steroids.pdf.

Related PFF Publications

- *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, Berin Szoka & Adam Thierer, Progress on Point 16.11, May 2009.
- *Written to Maine Legislature on Act to Protect Minors from Pharmaceutical Marketing Practices, LD 1677*, Berin Szoka, March 4, 2010.
- *Parental Controls & Online Child Protection: A Survey of Tools & Methods,* Adam Thierer, Special Report, Version 4.0, Fall 2008.
- *Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer*, Adam Thierer, Progress on Point 16.13, July 8, 2009.
- *The Perils of Mandatory Parental Controls and Restrictive Defaults*, Adam Thierer, Progress on Point 15.4, April 11, 2008.
- *Written Testimony before House Committee on the Judiciary on Cyber Bullying and other Online Safety Issues for Children*, Berin Szoka & Adam Thierer, Sept. 30, 2009.
- *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, Comments of Berin Szoka to FTC Exploring Privacy Roundtable, Nov. 2009.
- *Privacy Polls v. Real-World Trade-Offs*, Berin Szoka, Progress Snapshot 5.10, Oct. 2009.
- *Online Advertising & User Privacy: Principles to Guide the Debate*, Berin Szoka & Adam Thierer, Progress Snapshot 4.19, Sept. 2008.
- *Targeted Online Advertising: What's the Harm & Where Are We Heading?*, Berin Szoka & Adam Thierer, Progress on Point 16.2, April 2009.
- *How Financial Overhaul Could Put the FTC on Steroids & Transform Internet Regulation Overnight*, Berin Szoka, Progress Snapshot 6.7, March 2010.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
202-289-8928 ■ mail@pff.org ■ @ProgressFreedom ■ www.pff.org

THE PROGRESS & FREEDOM FOUNDATION

Response to Questions from Sen. Mark Pryor
by Berin Szoka
Senior Fellow, The Progress & Freedom Foundation
& Director of PFF's Center for Internet Freedom
www.pff.org

June 1, 2010

Regarding Hearing on
"An Examination of Children's Privacy: New Technologies
& the Children's Online Privacy Protection Act"

Before the
Subcommittee on Consumer Protection
Committee on Commerce, Science & Transportation
U.S. Senate, Held April 29, 2010

Thank you, Chairman Pryor, for the opportunity to supplement my written testimony from this hearing by responding to your questions.[1] In my responses, I have incorporated some of the material found in the comprehensive survey of the perils of expanding COPPA's scope beyond its original, limited purposes (what we have called "COPPA 2.0") that my colleague Adam Thierer and I published in May 2009: *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*.[2] Further detail on many of the points below can be found in that paper.

I. A Reexamination of COPPA

It bears repeating at the outset that the Federal Trade Commission's (FTC) current proceeding is not examining the Children's Online Privacy Protection Act ("COPPA") itself (the statute),[3] but rather the "COPPA Rule" (the regulations mandated by the agency pursuant to COPPA).[4] The agency is well aware of this distinction—and, indeed, far more precise about it than probably any interested party. For example, the agency's recent inquiry is titled "Request for Public

---

1 Written Testimony of Berin Szoka, Hearing on "An Examination of Children's Privacy: New Technologies & the Children's Online Privacy Protection Act" before the Subcommittee on Consumer Protection, Committee on Commerce, Science & Transportation, U.S. Senate, April 29, 2010, www.pff.org/issues-pubs/testimony/2010/2010-04-29-Szoka_Written_COPPA_Testimony.pdf.

2 Berin Szoka & Adam Thierer, *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, Progress on Point 16.11, May 2009, http://pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-verification.pdf ("*COPPA 2.0*").

3 15 U.S.C. §§ 6501-6506.

4 16 C.F.R. Part 312.

Comment on the Federal Trade Commission's *Implementation of the Children's Online Privacy Protection Rule*."[5] But it is a distinction that is far too often lost on many advocates who are lobbying for change.

Congress, of course, retains the authority to change the COPPA statue at any time, and it is well within the jurisdiction of this committee to consider doing so. But in re-examining COPPA, lawmakers should tread carefully. *Any attempts to reopen COPPA to expand the statute beyond its original, limited purposes could raise serious constitutional questions about the First Amendment rights of adults as well as older teens and site and service operators, and also have unintended consequences for the health of online content and services without necessarily significantly increasing the online privacy and safety of children.*

A. Do you think the age limit in COPPA is appropriate? And if so, why?

Yes, and understanding why is the key to understanding the delicate balance of COPPA in general. The COPPA Rule's requirements are *relatively* easy for site and service operators to implement, and for the government to enforce, because they apply only to the collection of information about children under 13 by commercial operators (or the public sharing of information by children themselves) only when (i) the operator's site or service is "directed to children" or (ii) the operator has actual knowledge that they are collecting personal information from a child. But the key practical difficulty in implementing a COPPA 2.0 system for adolescents 13 and above is in the anonymity inherent in the technical architecture of the Internet. To quote a memorable cartoon from *The New Yorker*: "On the Internet, nobody knows you're a dog."[6] Because website operators generally do not know who is accessing their site, requiring any special treatment of minors is tantamount to requiring age-verification of *all* users.[7] Again, COPPA's ingenious solution to this problem is that the law applies only to the limited "Internet Jr." of sites "directed at children," or in cases where an operator has "actual knowledge" that it is dealing with a child.

Because "child-oriented" websites are generally easy to define and are very rarely used by adults, COPPA's age verification mandate has not significantly impacted the free speech rights of adults because few adults other than parents ever want to use these sites, and parents essentially are already age verifying themselves in the process of providing "verifiable trial consent" for their children (those under 13). But it is *far* more difficult to define a class of "adolescent-oriented" websites (i.e., "directed at" kids age 13-17, as proposed in New Jersey in 2008[8]) that are not also used by significant numbers of adults. The practical result of such COPPA expansion efforts would be the same as simply specifying that a certain category of

---

5 Federal Trade Commission, *Children's Online Privacy Protection Rule: Request For Public Comment on the Federal Trade Commission's Implementation of the Rule*, 75 Fed. Reg. 17,089, April 5, 2010, http://www.ftc.gov/os/2010/03/100324coppa.pdf (*COPPA Implementation Review*).

6 Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, THE NEW YORKER, July 5, 1993, at 61, *available at* www.unc.edu/depts/jomc/academics/dri/idog.html (cartoon of a dog, sitting at a computer terminal, talking to another dog).

7 Of course, the COPPA's second prong of age-verification requirement applies only when the website operator has "actual knowledge" that the user is a minor. 16 C.F.R. § 312.3.

8 A.B. 108, Gen. Assem., 213th Leg. Sess. (N.J. 2008), www.njleg.state.nj.us/2008/Bills/A0500/108_I1.HTM.

websites (such as those with a public "wall," as proposed in Illinois in 2008[9]) must age-verify of a large number of adults to distinguish adults (who do not require verifiable parental consent) from children (who do require verifiable parental consent). This raises profound First Amendment concerns—particularly about the right of Americans to speak and receive information anonymously online.[10]

It was at least in part in recognition of the difficult First Amendment questions discussed below that Congress removed the requirement in the initial legislative draft of COPPA that would have required operators to "use reasonable efforts to provide the parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17."[11]

These First Amendment concerns are not conjectural: The courts have already struck down precisely this kind of broad age verification mandates—specifically, as found in the Children's Online Protection Act (COPA),[12] another 1998 law sometimes confused with COPPA. In essence, COPPA is focused on certain kinds of potentially harmful *contacts* while COPA is focused on potentially harmful *content*.[13] COPA attempted to prevent children from accessing material deemed "harmful to minors" by requiring all users attempting to access such content to provide a credit card, on the theory that only adults have credit cards. But the courts concluded that, "payment cards cannot be used to verify age because minors under 17 have access to credit cards, debit cards, and reloadable prepaid cards" and, although "payment card issuers usually will not issue credit and debit cards directly to minors without their parent's

---

9 H.B. 1312, 96th Gen. Assem., Synopsis as Introduced (Il. 2007) [hereinafter *SNWARA*], *available at* www.ilga.gov/legislation/billstatus.asp?DocNum=1312&GAID=10&GA=96&DocTypeID=HB&LegID=43038&SessionID=76.

10 *See infra* at 3-9.; *see generally, COPPA 2.0*, *supra* note 2; Adam Thierer, The Progress & Freedom Foundation, *USA Today, Age Verification, and the Death of Online Anonymity*, PFF Blog, Jan. 23, 2008, http://blog.pff.org/archives/2008/01/usa_today_doesn.html. 4

11 This requirement was contained in the original bill, Children's Online Privacy Protection Act, S. 2326, 105th Cong. § 3(a)(2)(A)(iii), (1998), but was removed when that bill was reintroduced in its final form. In the interim, Congress held a hearing at which testimony was offered by, among others, Deirdre Mulligan, on behalf of the Center for Democracy and Technology, which generally supported COPPA but argued for the very revisions that were ultimately made. In particular, Mulligan argued that:

> under the bill each time a 15 year old signs-up to receive information through email his or her parent would be notified. For example if a 15 year old visits a site, whether a bookstore or a women's health clinic where material is made available for sale and requests information about purchasing a particular book or merely inquires about books on a particular subject (abuse, religion) using their email address the teenager's parent would be notified. This may chill older minors in pursuit of information.

Testimony of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology, before the Senate Committee on Commerce, Science and Transportation Subcommittee on Communications, Sept. 23, 1998, http://web.archive.org/web/20080327000913/http://www.cdt.org/testimony/980923mulligan.shtml.

12 47 U.S.C. § 231.

13 COPA makes it illegal to "knowingly … make[] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." 47 U.S.C. 231.

consent because of the financial risks associated with minors… there are many other ways in which a minor may obtain and use payment cards."[14]

1. COPPA's Current Age Range Respects the First Amendment Rights of Adults

Besides the fact that credit cards were simply inadequate for proving that someone was not a child (a very different problem from obtaining verifiable parental consent, as discussed below), the court held that requiring adults to prove that they were not children by providing credit card information violated the First Amendment in a number of ways.

First, COPA burdened the speech rights of adults to access information subject to age verification requirements, both by making speech more difficult and by stigmatizing it. In 2003, the Third Circuit noted that age verification requirements "will likely deter many adults from accessing restricted content, because many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial."[15] In 2008, in striking down COPA for the third and final time, the Third Circuit approvingly quoted the district court, which had noted that part of the reason age verification requirements deterred users from accessing restricted content was "because Internet users are concerned about security on the Internet and because Internet users are afraid of fraud and identity theft on the Internet."[16] The Supreme Court has recognized the vital importance of anonymous speech in the context of traditional publication.[17] By imposing broad age verification requirements, COPPA 2.0 would restrict the rights of adults to send and receive information anonymously just as COPA did. If anything, the speech burdened by COPPA 2.0 deserves *more* protection, not less, than the speech burdened by COPA: Where COPA merely burdened access to content deemed "harmful to minors" (*viz*., pornography), COPPA 2.0 would burden access to material by adults as well as minors, not because that material is harmful or obscene, but merely because it is "directed at" minors! Thus, the content covered by COPPA 2.0 proposals could include not merely pornography, but communications of a political nature, which deserve the highest degree of First Amendment protection.

Second, COPA burdened the speech rights of operators because the necessary corollary of blocking adults from accessing certain content anonymously—and thereby deterring some users from accessing that content—is reducing the audience of those sites. Similarly, if COPPA's age ceiling were raised to cover adolescents, some websites would self-censor themselves to

---

[14] ACLU v. Gonzales, 478 F. Supp. 2d 775, 801 (E.D. Pa. 2007) [hereinafter *Gonzales*]. COPA would have prohibited the online dissemination of material deemed harmful to minors under 17 for commercial purposes, 47 U.S.C. § 231(a)(1), subject to a safe harbor for sites that made a "good faith" effort to restrict access by minors: "(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; (B) by accepting a digital certificate that verifies age; or (C) by any other reasonable measures that are feasible under available technology," 47 U.S.C. § 231(c)(1).

[15] ACLU v. Ashcroft, 322 F.3d 240, 259 (3d Cir. 2003) (*ACLU II*).

[16] ACLU v. Ashcroft, 534 F.3d 181, 196 (3d Cir. 2008) (*ACLU III*) (citing *Gonzales*, 478 F. Supp. 2d 775 at 806).

[17] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (striking down law that prohibited distribution of anonymous campaign literature); *see also* Talley v. California, 362 U.S. 60 (1960) (striking down a state law that forbade all anonymous leafletting).

avoid offering content they fear could be considered "directed at" adolescents because doing so might subject them to an age verification mandate for all users—or to legal liability if they failed to implement age verification. The substantial cost of age verification could significantly impact, if not make impossible, the razor-thin business models of many sites, which generally do not charge for content and rely instead on advertising revenues. The Third Circuit cited all of these burdens on the free speech rights of website operators in striking down COPA.[18]

Third, courts held that "[b]locking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them."[19] Similarly, parental control software already empowers parents to restrict their kids' access to websites and similar software is evolving for mobile services and smartphone software (*i.e.*, applications or "apps") that would offer parents control over what services kids use that allow them to share their personal information, either with operators or with other users.

Finally, it's worth noting that COPPA 2.0 would restrict the ability of adolescents to access content (in interactive contexts where they might also share personal information), not because it could be harmful to them or because it is obscene, but merely because it is "directed to" them. While the First Amendment rights of minors may not be on par with those of adults, adolescents *do* have the right to access certain types of information and express themselves in certain ways.[20] The Supreme Court has held that "constitutional rights do not mature and come into being magically only when one attains the state-defined age of majority."[21] It remains unclear how an expanded COPPA model might interfere with the First Amendment

---

[18] *See ACLU III*, 534 F.3d at 196-97 (citing *Gonzales*, 478 F. Supp. 2d 775 at 804). The Court held that websites "face significant costs to implement [COPA's age verification mandates] and will suffer the loss of legitimate visitors once they do so." *Id*. at 197.

[19] *Id*. at 198 (quoting *ACLU v. Mukasey*, 534 F.3d 181, 198 (2008)).

[20] *See* Theresa Chmara & Daniel Mach, *Minors' Rights to Receive Information Under the First Amendment*, Memorandum from Jenner & Block to the Freedom To Read Foundation, Feb. 2, 2004, www.ala.org/ala/aboutala/offices/oif/ifissues/issuesrelatedlinks/minorsrights.cfm (summarizing case law regarding minors' first amendment rights, especially in schools and in the context of mandates that public libraries filter Internet content); United States v. Am. Library Ass'n, 123 S. Ct. 2297 (2003), *available at* laws.findlaw.com/us/000/02-361.html (upholding the constitutionality of a filtering software system applicable to minors); *see generally*, Tinker v. Des Moines Ind. Comm. School Dist., 393 U.S. 503 (1969) (upholding students' rights to wear protest armbands and affirming that minors have speech rights), *available at* www.oyez.org/cases/1960-1969/1968/1968_21; *cf*. Morse v. Frederick, 551 U.S. 393 (2007), *available at* www.oyez.org/cases/2000-2009/2006/2006_06_278/ (holding that the First Amendment rights of students in school and at school-supervised events are not as broad as those of adults in other settings).

[21] Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 74 (1976) (minors' right to abortion). *See also Bellotti v. Baird*, 443 U.S. 622, 635 n.13 (minors possess close to the "full capacity for individual choice which is the presupposition of First Amendment guarantees"); Catherine Ross, *An Emerging Right for Mature Minors to Receive Information*, 2 U. PA. J. CONST. L. 223 (1999); Lee Tien & Seth Schoen, Reply Comments of the Electronic Frontier Foundation filed in *Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming*, MB Docket No. 0926, Federal Communications Commission, May 18, 2009, http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520216901.

rights of adolescents, but it is clear that privacy and speech rights would come into conflict under COPPA 2.0, as they do in other contexts.[22]

For example, how might the parental-consent based model limit the ability of adolescents to obtain information about "safer sex" or how to deal with trauma, depression, family abuse, or addiction? Would an abusive father authorize a teen to visit a website about how to report child abuse? Would parents of adolescents struggling with their sexual identity let their children participate in a self-help social networking page for gay and lesbian youth?[23] The rights are at play here are critically important and must be balanced carefully.

Preserving the ability of adolescents to participate in online interactions goes beyond content that most people would recognize as "serious"—from the perspective of both First Amendment values and the education of children. As a recent MacArthur Foundation study of the youth Internet use concluded:

> Contrary to adult perceptions, while hanging out online, youth are picking up basic social and technological skills they need to fully participate in contemporary society. Erecting barriers to participation deprives teens of access to these forms of learning. Participation in the digital age means more than being able to access "serious" online information and culture.[24]

Even if parents have an absolute right to block their adolescents' access to such data, they can better exercise that right by applying strict controls on the computers in their home. As discussed below, there are ways to encourage innovation in such parental empowerment tools without changing COPPA itself. But COPPA 2.0 proposals go well beyond recognizing parents' rights by by making parental consent a "default" requirement for adolescents to access a wide range of content—meaning that parents must "opt-in" on behalf of their children before their children can participate in sites and services covered by COPPA. This, in turn, burdens the ability of adolescents to communicate, because their parents might censor (rightly or wrongly) certain information, or simply fail to understand the technologies involved or be responsive to the opt-in requests when their kids want to access a new interactive site or service. But

---

[22] *See generally* Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97 (2000), *available at* http://law.fordham.edu/publications/articles/200flspub6588.pdf; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You,* 52 STAN. L. REV. 1175 (2000), *available at* www.law.ucla.edu/volokh/privacy.htm.

[23] "There are parents who, for a variety of reasons (political, cultural, or religious beliefs, ignorance of the facts, fear of being exposed as abusers, etc.), would deliberately prevent their teens from accessing social-network sites (SNS)." Internet Safety Technical Task Force, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*, Dec. 31, 2008, Appendix F, Statement of Connect Safely, at 262, http://cyber.law.harvard.edu/pubrelease/isttf (listing examples of unintended consequences of age verification mandates) [hereinafter *ISTTF Final Report*]. Full disclosure: Adam Thierer was a member of this task force.

[24] John D. and Catherine T. MacArthur Foundation, *Living and Learning with New Media: Summary of Findings from the Digital Youth Project*, at 2 [hereinafter *MacArthur Study*] http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf.

whatever the free speech rights of adolescents, if anyone should be interfering with those rights, it should be their parents—not the government.

2. COPPA's Current Age Range Allows Beneficial Communication between Adolescents & Adults

Finally, COPPA 2.0 could infringe on the free speech rights of adults to communicate with adolescents online by driving operators to segregate users by age or to attempt to block access by adolescents. As explained below, for the sake of marginal (if any) gains in child protection, we would be excluding *beneficial* interaction between adults and minors.

The vast majority of online interactions between adults and minors are not of a harassing, predatory or otherwise harmful nature—indeed, they generally involve adults looking to help or assist minors in various ways. As the MacArthur Foundation study cited above concluded:

> In contexts of peer-based learning, adults … have an important role to play, though it is not the conventionally authoritative one. In friendship-driven practices, direct adult participation is often unwelcome, but in interest-driven groups we found a much stronger role for more experienced participants to play. Unlike instructors in formal educational settings, however, these adults are passionate hobbyists and creators, and youth see them as experienced peers, not as people who have authority over them. *These adults exert tremendous influence in setting communal norms and what educators might call "learning goals," though they do not have direct authority over newcomers.*[25]

A substantial portion of those interactions involve parents talking to their own kids, older and younger siblings communicating with one another, teachers and mentors talking to their students, or even co-workers of different ages communicating. Even when adult-minor communications involve complete strangers, there is typically a socially-beneficial purpose. Examples include debating politics on a discussion board, or collaboratively editing a Wikipedia entry, or communicating and collaborating on a common purpose on a presidential campaign website involving millions of volunteers of all ages. There are countless other examples. Such interactions could be severely curtailed by COPPA 2.0 proposals. Restricting such interactions would raise profound First Amendment concerns about freedom of speech as well as of association.

In any First Amendment analysis, a court must consider not only the free speech rights at stake and the availability of less restrictive alternatives to regulation, but the governmental interest being advanced. Again, neither COPPA nor the COPPA 2.0 proposals recently contemplated at the state level require exclusion of older users from a website, nor directly govern the sharing of personal information among users (where that sharing does not also constitute collection by the site itself). But separation of adolescents from adults is likely to be an indirect effect of COPPA 2.0 requirements—as COPPA 2.0 advocates probably realize—because, once operators are required to age-verify users, they will face reputational, political and potentially legal pressure to make interactions between adolescents and children more difficult in the name of

---

[25] *MacArthur Study*, *supra* note 24, at 2.

"child safety." More subtly, if site operators have an incentive to avoid having their sites be considered "directed at" adolescents, they will also have an incentive to discourage adolescent participation on their sites—which achieves a similar result.

Given the lack of strong identity records for minors, it's much easier for an adult to pretend to be a minor than vice versa. Thus, one must further ask if attempting to quarantine children from adults (however indirectly) actually advances, on net, a strong governmental interest in child protection. Such a quarantine is unlikely to stop adults with truly nefarious intentions from communicating with minors, as systems designed to exclude participation by adults in a "kids-only" or "adolescents-only" area can be easily circumvented. The effect of age stratification on truly bad actors is likely to be marginal at best—or harmful at worst: Building walls around adolescents through age-verification might actually make it *easier* for predators to target teens, since a predator who gains access to a supposedly teen-only site will be *less* likely to be exposed as a predator than by targeting an adult the predator thinks is a teen.

To hear some of the advocates of COPPA expansion talk about how teens currently behave online, one might think that online environments in which adolescents were left to their own devices—imagine a "Teen MySpace" for the 13-17 crowd, walled off from the rest of MySpace—would be far worse, perhaps an online version of *Lord of the Flies*. These concerns are clearly exaggerated: The critics frequently complain about "the way kids talk to each other these days" while looking at their own past adolescent banter with rose-tinted glasses. What *is* clear is that adolescents (and young adults) behave *better* in online environments where adults are present, too. Perhaps the best demonstration of this fact has been the uproar from adolescents and young adults that has accompanied Facebook's explosive growth in popularity among older users.[26] Many kids hate the idea of adults joining Facebook precisely because the presence of adults encourages kids to "self-regulate" by exercising better judgment and following better netiquette.[27]

Anne Collier, founder and executive director of the child safety advocacy organization Net Family News, Inc. and editor of NetFamilyNews.org and ConnectSafely.org, suggests that the push for "segregation" by age (*e.g.*, creating a teen-only version of Second Life) for safety's sake is "losing steam" because:

> It's a response to the predator panic teens and parents have been subjected to in U.S. society, not to the realities of youth on the social Web. What nearly a decade of peer-reviewed academic research shows is that peer-to-peer behavior is the online risk that affects many more youth, the vast majority of online kids

---

[26] Justin Smith, *Number of US Facebook Users Over 35 Nearly Doubles in Last 60 Days*, Inside Facebook Blog Mar. 25, 2009, www.insidefacebook.com/2009/03/25/number-of-us-facebook-users-over-35-nearly-doubles-in-last-60-days/.

[27] *See e.g.*, Lori Aratani, *When Mom or Dad Asks To Be a Facebook "'Friend,"* THE WASHINGTON POST, Mar. 9, 2008, www.washingtonpost.com/wp-dyn/content/article/2008/03/08/AR2008030801034.html. "'I do not know if this has happened to anybody, but this morning I log on to Facebook and I have a new friend request!' wrote 19-year-old Mike Yeamans, a sophomore at James Madison University, on one of several 'No Parents on Facebook' groups that have popped up on the site. 'I am excited to make a new friend so I click on the link. I could not believe what I saw. My father! This is an outrage!'" *Id*.

> who are not already at-risk youth offline. Segregating teens from adults online doesn't address harassment, defamation, imposter profiles, cyberbullying, *etc*. It may help keep online predators away from kids (even though online predation, or abuse resulting from online communication, constitutes only 1% of overall child sexual exploitation…), which is a great outcome, but it's not enough unless all that parents are worried about is predators.[28]

Of course, adults play a critical role in disciplining interaction among the 0-12 age bracket, but not as direct participants in on-site interaction. Again, how many adults actually want to use Club Penguin, a site clearly geared toward the Net's youngest users? Instead, parents can supervise what their kids do online through parental control software. Parents could, of course, use that same software to monitor what their adolescent kids do, too. But as kids get older, most parents realize that the training wheels have to come off at some point. Few parents will want to spy on their 17-year old until the day before the kid starts college (or enlists in the military or gets married). But most parents probably *would* prefer that, if their kids are interacting in an online environment, they think twice about what they do and say online. It is by no means clear that restricting online interaction between teens and adults will serve that end.

B. Do you think COPPA should be strengthened?

I have seen no evidence of a need for Congress to reopen COPPA, and to the extent that some changes may be necessary in the implementation of COPPA, I believe the statute affords the FTC great flexibility in its definition of "Internet," as discussed below, as well as in allowing the agency to update the definition of "personal information." Thus, while there may be ways to improve implementation of the statute, I do not see a need for changing COPPA itself today.

Moreover, Congress must be cognizant of the downsides of reopening COPPA and – to the extent it is expanded along the lines some of have advocated—raising the prospect of the entire law being struck down as unconstitutional because it essentially converges with COPA, as Adam Thierer and I have explained in our work.[29] Again, COPPA is one of the few Internet laws Congress has passed over the last 15 years that was not challenged, blocked from taking effect, or overturned.

---

[28] Anne Collier, *Where Will OnlineTeens Go Next?*, May 1, 2009, www.netfamilynews.org/2009/05/where-will-online-teens-go-next.html (internal citations omitted). For evidence of at-risk youth, Collier sites the *ISTTF Final Report*, *supra* note 47. Regarding the percentage of all child sexual exploitation that results from online communication, she cites Janis Wolak, David Finkelhor & Kimberly Mitchell, Crimes Against Children Research Center, *Trends in Arrests of Online Predators*, 2009) www.unh.edu/ccrc/pdf/CV194.pdf; *see also*, Anne Collier, *Major Update on Net predators: CACRC study*, March 31, 2009, www.netfamilynews.org/2009/03/major-update-on-net-predators-mostly.html (summarizing study).

[29] *See generally supra* note 2.

C. Should the FTC reexamine what constitutes "personal information" in its review of COPPA? Or do you believe that the online space and the definition of personal information should remain the same as it was when the law was created over 10 years ago?

As I noted in my testimony, COPPA already gives the FTC the flexibility to update the definition of "personal information" to include "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[30] Because the definition of personal information also includes "information concerning the child or the parents of that child that the website collects online from the child and combines with [any of these identifiers]," the statute already covers essentially all information tied to a particular user where it is possible to contact that user. This dynamic definition is broad enough to keep pace with technological change because it is not simply a static listing of the "personal information" that was at issue in the late 1990s. For example, if the lodestar of "personal information" is the ability to contact a child, instant messaging screen names or social networking pseudonyms might qualify as "personal nformation." In your opinion, what is the biggest threat to children's privacy and safety in today's online world?

The biggest threat to children's online privacy and safety has always been, and will likely remain, the ignorance and naïveté that necessarily comes with youth. Though children may be quite technologically adept, far more so than many parents, they still lack the real-world experience necessary to appreciate the potential privacy and safety implications of heedlessly giving personal information away to site operators or, especially, making personal information publicly available to other Internet users. No amount of Federal legislation or regulation is going to keep children from divulging personal information if they aren't aware of its dangers. So, as discussed below, if a lack of knowledge or sophistication is the problem, the primary answer must be education, education and more education, not regulation, regulation, and more regulation.[31]

D. What do you think is the most urgent update to COPPA needed?

Again, the FTC should remove any doubt about the fundamental technological agnosticism of COPPA's potential coverage (actual coverage depending on whether, in any particular context, "collection" occurs and whether the site is directed at children or the operator has actual knowledge that it is "collecting" personal information from a child). The FTC should also encourage the development of mechanisms for verifying parental consent appropriate to these technologies, either by recognizing additional mechanisms or through certifying innovative safe harbor operators. Congress could direct, and fund, the FTC to conduct more education about COPPA, online privacy and online safety.

E. In your opinion, what would constitute the most appropriate definition of "sensitive data" in the context of children's online privacy?

COPPA already includes an excellent list of personal information:

---

[30] 15 U.S.C. § 6501(8)(F).

[31] *See infra* at III.A.4.

(A) a first and last name;
(B) a home or other physical address including street name and name of a city or town;
(C) an e-mail address;
(D) a telephone number;
(E) a Social Security number;[32]

As I noted in my testimony, COPPA already gives the FTC the flexibility to update the definition of "personal information" to include "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[33] Because the definition of personal information also includes "information concerning the child or the parents of that child that the website collects online from the child and combines with [any of these identifiers]," the statute already covers essentially all information tied to a particular user such that it is possible to contact that user. Thus, there should be no need to specify additional categories of sensitive data to achieve COPPA's purposes.

F. You said in your written testimony that a "COPPA expansion would undermine privacy." Would you mind explaining to the Committee your meaning?

Sites that implement age verification technologies (even through COPPA's "verifiable parental consent" loose form of age verification) require users to share personal information about themselves. Specifically, adults attempting to access sites behind an age verification wall would have to provide information adequate to establish that they are not, in fact, younger than whatever the higher age threshold of COPPA 2.0 might be. Similarly, children attempting to access such sites would have to provide information about themselves and their parents sufficient to establish the parent-child relationship so that a site can reasonably evaluate documentation purporting to establish "verifiable parental consent." Both forms of age verification (by adults, and by children/parents) could be accomplished by a number of means, but seem to be most commonly done today through use of a credit card.

Today, because COPPA requires age verification only for sites "directed at" children under 13 (or, in cases where an operator has "actual knowledge" that a particular user is under 13), the law in practice requires only the second sort of age verification. But if COPPA were expanded to cover, say, all sites "directed at" adolescents (however defined), the law would very likely require certain website operators to presume that *all* their users might be "children" whose parents' "verifiable parental consent" must be obtained prior to collection. This, in turn, would mean that large numbers of adults would, for the first time since COPA, be required by law (or at least, the website operator's interpretation of the law, which might tend to err on the side of caution) to age verify significant numbers of adults. As discussed below, this creates a significant burden on the First Amendment rights of adults to anonymous communication through interactive services that could allow public sharing of personal information. This would also significantly burdens website operators whose audience might be reduced by the apprehension caused by age verification mandates among users worried about having to

[32] 15 U.S.C. § 6501(8)(A-E).

[33] 15 U.S.C. § 6501(8)(F).

provide information for certification purposes or simply by the hassle of having to do so. In both respects, COPPA 2.0 would raise precisely the same constitutional problem that caused the courts to strike down COPA (but that are not raised by COPPA 1.0).[34]

But such an expansion of COPPA's age scope would also undermine privacy by requiring the sharing of more personal information in order to age-verify newly covered users. The same would be true of any attempts to expand COPPA by specifying that it applies to certain categories of websites (effectively disposing of the law's "directed at" analysis*). Thus, the irony of COPPA expansion is that lawmakers would be applying a law that was meant to protect the privacy and personal information of children to gather a great deal more information about kids, their parents, and many other adults.*

As the district court that struck down COPA noted:

> Requiring users to go through an age verification process would lead to a distinct loss of personal privacy. Many people wish to browse and access material privately and anonymously, especially if it is sexually explicit. Web users are especially unlikely to provide a credit card or personal information to gain access to sensitive, personal, controversial, or stigmatized content on the Web. As a result of this desire to remain anonymous, many users who are not willing to access information non-anonymously will be deterred from accessing the desired information.[35]

The same is true even for non-explicit material, such as would be covered by COPPA if the law's age range were expanded.

G. Do you support the FTC's review of COPPA? Do you believe it is necessary?

Yes, the FTC was well within its general operating procedures to accelerate its review of the COPPA Rules from 2015, the originally set date, to this year,[36] and it made sense for the agency to do so, given the pace of change in this area. In particular, it appears from comments made by many in industry that the FTC needs to do more to make clear that COPPA is, by original Congressional design, platform-agnostic, applying to any "collection" (including publication or sharing by users themselves) of "personal information" through a website or online service—*regardless of the device used to access that site or service*.

H. If you oppose expanding COPPA, do you believe it is working properly? Do you believe it is sufficient to protect children's privacy?

The original goals of COPPA, as expressed by its Congressional sponsors, were to:

---

[34] See supra at 3-9.

[35] *Gonzales*, 478 F. Supp. 775, 805 (E.D. Pa. 2007).

[36] *See* Federal Trade Commission, Staff Report, *Beyond Voice: Mapping the Mobile Marketplace*, April 2009, at 3, www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf ; *see also* FTC Operating Manual, § 7.5, at 33, http://www.ftc.gov/foia/ch07rulemaking.pdf (The FTC "has adopted a policy of reviewing each of its legislative rules (i.e. trade regulation rules and rules promulgated under special statutes) at least once every ten years.").

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[37]

Thus, as its name implies, COPPA is generally concerned with protecting the privacy of children. But COPPA's primary means for achieving this goal is enhancing parental involvement or, as the FTC has put it, "provid[ing] parents with a set of effective tools… for becoming involved in and overseeing their children's interactions online."[38] However admirable, "protect[ing] the safety of children" is merely an *indirect* goal of COPPA—something to be achieved through the means of enhancing parental involvement (COPPA's *direct* goal).

Viewed in this light, COPPA has probably been about as successful as could be expected given the fundamental technical reality of the Internet: In general, users and operators cannot, across the essentially infinite expanse of the digital chasm, definitively know how old other users are or even who they are.

The FTC asserts COPPA "has provided a workable system to help protect the online safety and privacy of the Internet's youngest visitors."[39] Yet many of those advocating expansion of COPPA do so on the grounds that COPPA makes children safer from sexual predators. What these advocates fail to acknowledge is that, to the extent COPPA has enhanced child safety—indeed, to the extent that COPPA can be effectively administered at all—it is because of the unique circumstances of the under-13 age bracket and the operators that have evolved to serve that community. In particular:

1. The functionality of child-oriented sites is usually tightly limited: They arewalled gardens;
2. Many smaller websites catering to children charge a fee for admission—even as fee-based models have withered away on the rest of the Internet; and
3. There are relatively few sites that cater exclusively to the under-13 crowd, which may be an unintended consequence of COPPA itself.

---

[37] 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

[38] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* at 28, Feb. 2007, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf (*2007 COPPA Implementation Report*).

[39] *Id*. at 28.

I. Would you support any changes to the rule or to the statute?

I would support changes to the statute if:

1. It were shown that those changes were necessary to prevent a demonstrable and substantial harm (not just a fear of potential harm), were narrowly tailored to that harm, and were the least restrictive means available for addressing that harm;
2. Those changes could reduce the difficulty and expense of complying with COPPA, thus promoting competition in the marketplace for children's content and services; or
3. Those changes could further empower parents to make decisions about their children's participation in online sites and services, without unduly burdening those sites and services.

But as explained throughout, I believe the FTC already has the tools it needs under COPPA in its current form. If the FTC needs anything more from Congress, it might be additional funding for educational efforts, encouraging new safe harbor programs, and targeted enforcement.

II. Privacy Implications of New Technologies

A. You said in your written statement, "the reality is that the technology for reliable age verification simply doesn't exist." Could it exist in the future? If your claim is valid, does that mean the business community, the FTC or Congress should not strive to find enhanced age verification methods?

In a February 2007 report to Congress about the status of COPPA and its implementation, the FTC said that no changes to COPPA were then necessary because the law had "been effective in helping to protect the privacy and safety of young children online."[40] In discussing the effectiveness of the parental consent verification methods authorized in the FTC's sliding scale approach, however, the agency acknowledged that "none of these mechanisms is foolproof."[41] The FTC attempted to distinguish these parental consent verification methods from other kinds of age verification tools in noting that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms."[42] This makes it clear that the FTC does not regard the methods the agency has prescribed for obtaining parental consent under COPPA as equivalent to strict age verification.

After years of searching for a technological "silver bullet," especially by state attorneys general, the practical limitations and dangers of age verification mandates are now widely recognized. Few continue to argue for directly mandating verification of the age of minors online—or that such verification, in its strictest sense, is even technically feasible. Federal courts have found that there is "no evidence of age verification services or products available on the market to owners of Web sites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by

---

[40] *Id.*, at 1.

[41] *Id*. at 13.

[42] *Id*. at 12.

a minor."[43] Few public databases exist that could be referenced to conduct such verifications for minors, and most parents do not want the few records that *do* exist about their children (*e.g.*, birth certificates, Social Security numbers, school records) to become more easily accessible.[44] Indeed, concerns about those records being compromised or falling into the wrong hands have led to legal restrictions on their accessibility.[45]

There are a host of other concerns about age verification mandates.[46] Some of these concerns were summarized in a recent report produced by the Internet Safety Technical Task Force, a blue ribbon task force assembled in 2008 by state attorneys general to study this issue:

> Age verification and identity authentication technologies are appealing in concept but *challenged in terms of effectiveness*. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues.[47]

But even if far more robust age verification solutions could be developed, they would not solve the central constitutional problem faced by efforts to expand COPPA's age range or scope of sites otherwise covered by COPPA regardless of age. This is because, in essence, the practical challenge under COPPA is not that children have to prove that they are in fact *under* a certain age, but two far more complicated problems.

First, once the verifiable parental consent requirement is triggered, either because a site is "directed at" children or because the operator knows that a particular user is a child (for example, because they have volunteered the fact that they are under 13 years old), the operator must make a "reasonable effort (taking into consideration available technology)" to

---

43 *Gonzales*, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007).

44 *See* Adam Thierer, The Progress & Freedom Foundation, *Age Verification Debate Continues; Schools Now at Center of Discussion*, PFF Blog, Sept. 25, 2008, http://blog.pff.org/archives/2008/09/age_verificatio_1.html.

45 Various laws and regulations have been implemented that shield such records from public use, including various state statutes and the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

46 For a fuller exploration of these issues, *see* Adam Thierer, The Progress & Freedom Foundation, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions*, Progress on Point No. 14.5, Mar. 2007; Adam Thierer, The Progress & Freedom Foundation, *Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General*, Jan. 14, 2008, www.pff.org/issues-pubs/other/090114ISTTFthiererclosingstatement.pdf; Nancy Willard, *Why Age and Identity Verification Will Not Work—And is a Really Bad Idea*, Jan. 26, 2009, www.csriu.org/PDFs/digitalidnot.pdf; Jeff Schmidt, *Online Child Safety: A Security Professional's Take*, The Guardian, Spring 2007, www.jschmidt.org/AgeVerification/Gardian_JSchmidt.pdf.

47 *ISTTF Final Report*, *supra* note 23, at 10.

verify parent-child relationship to ensure that adequate notice is given to, and authorization is obtained from, someone who is in fact the parent of that child.[48] This is more complicated than simply verifying the age of any particular user, and the statute's flexibility in exactly how operators are to fulfill this requirement is indicative of the difficulty involved.

Second is the very different problem of trying to ensure that a particular user is *not* a child. This is essentially the problem faced by COPA, where the solution was simply to require certain kinds of websites to age verify all users. Again, that solution is clearly unconstitutional, even though the material at issue was that deemed "harmful to minors" (increasing the government's interest in regulating communications). COPPA's ingenious way of sidestepping this problem is to limit broad verification mandates to sites that are "directed at" children or to situations where the operator has "actual knowledge" that a user is a child. (Furthermore, the verification required by COPPA is fundamentally different, being verification of "verifiable parental consent" rather than of the actual identity or age of a user.) This difference is profound, because it means that COPPA, in its present form, does not subject significant numbers of adults to age verification mandates. But, again, if the COPPA framework were expanded to cover older children or certain websites based on their functionality, COPPA would essentially converge with COPA by requiring large numbers of users to prove a negative: that they are *not* children.

It is difficult to see how that problem can ever be solved because even if there were a reasonably reliable solution for authenticating a user's identity, the constitutional analysis does not hinge on the accuracy of age or identity verification mechanisms, but on the chilling effects caused by government mandates that users provide more information about themselves than they otherwise would have to do in order to access certain interactive sites or services (that could potentially allow sharing of personal information). Simply put, this does not appear to be a problem that can be solved by any amount of technological innovation.

III. Policy Recommendations

A. What should the FTC or Congress do to strengthen children's safety and privacy online in conjunction with advanced technologies and mobile devices?

1. The FTC Should Clarify COPPA's Technological Breadth

As noted above, te FTC should remove any lingering doubt that COPPA is platform-agnostic. While new technologies may indeed present unique challenges and opportunities for "enhancing parental involvement" in the online activities of children, it should be uncontroversial and clear to everyone that COPPA applies to any technology that facilitates the "collection" of personal information over the Internet (which, again, means not only collection by operators for advertising or other purposes but also simply enabling users to make personal information publicly available). This is simply the plain reading of the statute. COPPA defines the key term "Internet" broadly to mean:

> collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-

[48] *See* 16 C.F.R. § 312.1 (definition of "Obtaining verifiable consent").

> wide network of networks that employ the Transmission Control Protocol/ Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.[49]

In its 1999 COPPA rulemaking, the Commission declared that:

> The proposed Rule's definition of ''Internet'' made clear that it applied to the Internet in its current form and to any conceivable successor. Given that the technology used to provide access to the Internet will evolve over time, it is imperative that the Rule not limit itself to current access mechanisms.[50]

The Commission rejected a commenter's suggestion that the agency "clarify that the definition 'clearly includes networks parallel to or supplementary to the Internet such as those maintained by the broadband providers… [and] intranets maintained by online services which are either accessible via the Internet or have gateways to the Internet.'" The Commission concluded that its "definition of 'Internet' was [already] sufficiently broad to encompass such services and adopts that definition in the final Rule.[51] The Commission has subsequently incorporated this language into its FAQ, which serves as its primary interpretive guide for those interested in understanding application of the rule (especially small site operators):

> The Rule's Statement of Basis and Purpose makes clear that the term Internet is intended to apply to broadband networks, as well as to intranets maintained by online services that either are accessible via the Internet, or that have gateways to the Internet.[52]

As a matter of statutory construction, this interpretation is probably correct and would probably receive deference from a court under the *Chevron* doctrine if challenged.[53] This interpretation would allow the FTC to apply COPPA's requirements to services like text messaging and Massively Multiplayer Online (MMO) games like World of Warcraft and Second Life that are "accessible via the Internet," regardless of the device used to access them.

2. The FTC Should Promote Flexibility in COPPA Compliance

The FTC should take into consideration the unique challenges and opportunities raised by new devices and services in deciding how to implement COPPA. Alternative means of establishing verifiable parental consent may work much better for the technologies, devices, and services of tomorrow, and the FTC will probably hear in great detail about this issue at its roundtable and in comments filed in response to its Implementation Review. In deciding how to respond to

---

[49] 15 U.S.C. § 6501(6).

[50] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,891 (Nov. 3, 1999), *available at* www.ftc.gov/os/1999/10/64fr59888.pdf

[51] *Id*.

[52] Federal Trade Commission, *Frequently Asked Questions about the Children's Online Privacy Protection Rule*, Question 6 ("What types of online transmissions does COPPA apply to?"), www.ftc.gov/privacy/coppafaqs.shtm

[53] *Chevron U.S.A., Inc. v. Natural Res. Defense Council, Inc*., 467 U.S. 837 (1984) (required federal courts to defer to an agency's interpretation of a statute, so long as the interpretation was "reasonable")..

those suggestions, the FTC should aim to maximize the flexibility available to online operators to comply with COPPA, and to simplify the process wherever possible for parents and children. Where parents have already given effective consent for their children to use a particular service—for example, by paying for a text message plan as part of the monthly service for a cell phone—there may be no need to impose additional requirements because COPPA's goal of "enhancing parental involvement" through parental consent has already been achieved. More granular controls (say, blocking texting to a particular number) may be quite valuable to parents but they are probably beyond the purview of COPPA and, in any event, are already being offered by many service providers in response to parental demand.[54] This suggests the marketplace is already working to empower parents, which is, after all, COPPA's primary purpose.

In particular, the FTC could use the discretion afforded to it by the statute to certify more "safe harbor" operators, whose self-regulatory guidelines would be deemed to be sufficient to establish compliance with COPPA. For example, as children under 13 increasingly have their own ever more sophisticated mobile phones,[55] wireless carriers and mobile operating system developers might collaborate on a standardized system that requires verifiable parental consent upon the initial purchase of a mobile phone service plan or addition of certain options, like text messaging or data service but that also provides parents control over which applications their children install on their phones. Such a system might work by, for instance, giving parents a password-protected account upon the initial verification of their consent for the service plan, and then allowing them to easily grant consent for their children to install applications in the future, keep track of those applications for which they have already granted consent, access information collected by those applications, review the privacy policies of those applications, or revoke their consent as they see fit. Such a system is, at least in theory, exactly what policymakers should aim to enable, but it may should be *required* by COPPA. The ultimate goal should be to encourage companies to empower parents to manage, as easily as possible, their children's participation in online activities that could entail the sharing of personal information—which is what parents are already demanding in the marketplace. But such a highly complex system should be designed and managed by the private sector, not the government, and this is precisely what the safe harbor program provided for by COPPA would allow the FTC to do to the extent consistent with COPPA's scope.

Concretely, lawmakers might encourage the FTC to issue a call to industry for new safe harbor proposals, to work with industry to support the development of these proposals, and then perhaps issue a consolidated notice about these proposals in order to expedite the notice and comment process required by the statute before the agency may grant approval to any new

---

[54] *See, e.g.,* Verizon Wireless, Usage Controls, https://wbillpay.verizonwireless.com/vzw/nos/uc/uc_home.jsp (describing parental control tools available to parents including blocking numbers, time restrictions and usage filters); https://wbillpay.verizonwireless.com/vzw/nos/uc/uc_content_filter.jsp (content filters); *see generally* http://parentalcontrolcenter.com/#_self; http://www.wireless.att.com/learn/articles-resources/parental-controls/index.jsp; http://shop.sprint.com/en/services/safety_security/parental_control.shtml.

[55] Amanda Lenhart, Rich Ling, Scott Campbell, Kristen Purcell, *Teens and Mobile Phones*, April 20, 2010, http://www.pewinternet.org/Reports/2010/Teens-and-Mobile-Phones.aspx.

safe harbor program. More such suggestions will, no doubt, come out of the COPPA Roundtable and comments, and Congress should encourage the FTC to heed such suggestions.

Or, the FTC could, as the Implementation Review contemplates, allow operators, at least in some circumstances, to use "an automated system of review and/or posting" to satisfy the existing "deletion exception to the definition of collection."[56] In other words, sites could potentially allow children to communicate with each other through chat rooms, message boards, and other social networking tools *without* having to obtain verifiable parental consent if they had in place algorithmic filters that would automatically detect personal information such as a string of seven or ten digits that seems to correspond to a phone number, a string of eight digits that might correspond to a Social Security number, a street address, a name, or even a personal photo—and prevent children from sharing that information in ways that make the information "publicly available." Such a technology would, of course, not be foolproof, and might be circumvented by children smart enough to find other ways to share information that the algorithm will prevent them from sharing. Yet despite these limitations, the FTC should encourage the development of such technologies because they could allow sites to meet COPPA's central goal of limiting the sharing of information that could allow the contacting or identification of a child *without* going through COPPA's intentionally (or at least, necessarily) cumbersome parental consent verification procedures. This would benefit kids and operators alike by facilitating communication with less risk to children's online privacy or safety.

3. Enhanced Enforcement Is Generally Preferable to Expanded Regulation

Besides promoting empowerment solutions, the FTC should of course be vigilant about a second "E-word": *enforcement*. As a general matter, before rushing to change an existing regulatory regime or give an agency new powers, Congress should always ask whether the laws on the books are being given a chance to succeed. Specifically, Congress should consider whether the FTC has the staffing, technological and financial resources it needs to enforce COPPA's requirements effectively.

4. Education is Vitally Important

Finally, the FTC should be encouraged—and funded—to make maximum use of the final "E-word": *education*. We can and should provide parents with more and better tools to make informed decisions about media and communications tools in their lives and the lives of their children. But technical tools can only supplement—they can never supplant—education, parental guidance, and better mentoring. Education and mentoring are the most essential part of the solution to concerns about online child privacy and safety. We can, and must, do more as parents and as a society to guide our children's behavior and choices online. The FTC has a track record of great success in this area, including:

- OnGuard Online, the website intended to educate all Internet users about online safety
- NetCetera, the FTC's excellent child safety effort
- The "You Are Here" virtual mall launched by the FTC last year to educate kids in 5th-8th grade (ages 10-14) about marketing both online and offline.

---

[56] COPPA Implementation Review, *supra* note 5, Question 9a.

- AdMongo, a game-tutorial website intended to teach kids about advertising and marketing, both online and offline, to help them become smarter consumers. The service includes a discussion of how information is used for advertising purposes online.

In addition, Congress could fund a number of grants for educational efforts intended to educate kids and parents about online privacy and safety. This approach is exemplified by Rep. Wasserman Schultz's currently pending "Adolescent Web Awareness Requires Education Act (AWARE Act)" (H.R. 3630), which would create a education grant program to address issues of cybercrime affecting children, including cyber bullying, in schools and communities.[57] Indeed, The "Protecting Children in the 21st Century Act," which was signed into law by President Bush in 2008 as part of the "Broadband Data Services Improvement Act,"[63] required that the Federal Trade Commission (FTC) "carry out a nationwide program to increase public awareness and provide education" to promote safer Internet use and:

> utilize existing resources and efforts of the Federal Government, State and local governments, nonprofit organizations, private technology and financial companies, Internet service providers, World Wide Web-based resources, and other appropriate entities, that includes (1) identifying, promoting, and encouraging best practices for Internet safety; (2) establishing and carrying out a national outreach and education campaign regarding Internet safety utilizing various media and Internet-based resources; (3) facilitating access to, and the exchange of, information regarding Internet safety to promote up to-date knowledge regarding current issues; and, (4) facilitating access to Internet safety education and public awareness efforts the Commission considers appropriate by States, units of local government, schools, police departments, nonprofit organizations, and other appropriate entities.[64]

Education-based approaches are vital because they can help teach kids how to behave in—or respond to—a wide variety of situations. Education teaches lessons and builds resiliency, providing skills and strength that can last a lifetime. That was the central finding of a blue-ribbon panel of experts convened in 2002 by the National Research Council of the National Academy of Sciences to study how best to protect children in the new, interactive, "always-on" multimedia world. Under the leadership of former U.S. Attorney General Richard Thornburgh, the group produced a massive report that outlined a sweeping array of methods and technological controls for dealing with potentially objectionable content and online dangers. Ultimately, however, the experts used a compelling metaphor to explain why education was the most important strategy on which parents and policymakers should rely:

> Technology—in the form of fences around pools, pool alarms, and locks—can help protect children from drowning in swimming pools. However, teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning. Does this mean that parents should not buy fences, alarms, or locks? Of course not—because

---

[57] Adolescent Web Awareness Requires Education Act, H.R. 3630, 111th Cong. (2009), *available at* www.opencongress.org/bill/111-h3630/show.

> they do provide some benefit. But parents cannot rely exclusively on those devices to keep their children safe from drowning, and most parents recognize that a child who knows how to swim is less likely to be harmed than one who does not. Furthermore, teaching a child to swim and to exercise good judgment about bodies of water to avoid has applicability and relevance far beyond swimming pools—as any parent who takes a child to the beach can testify.[58]

Regrettably, we often fail to teach our children how to swim in the "new media" waters. Indeed, to extend the metaphor, it is as if we are generally adopting an approach that is more akin to just throwing kids in the deep end and waiting to see what happens. Educational initiatives are essential to rectifying this situation.

B. Do you agree with the direction the FTC is taking as it reexamines the implementation and effectiveness of COPPA?

It's still probably too early to say with any certainty what that direction is—especially on the eve of the FTC's COPPA Roundtable. In general, I am encouraged by the tone of the FTC's official statements in this proceeding, and also by the oral statements of FTC staff at recent events. They appear to have a healthy understanding of the limitations as well as the advantages of COPPA, as well as a healthy sensitivity to the potential effects on the competitiveness of the landscape for children's content and services.

I'm particularly encouraged to see that the implementation review begins by asking about the ongoing need for the rule, its costs and benefits, and its unintended effects. This is precisely the right way to begin any inquiry into the implementation of regulations. COPPA has undoubtedly succeeded in its primary goal of enhancing parental involvement in their child's online activities in order to protect the privacy and safety of children online.[59] Yet these benefits have come at a price, since the costs of obtaining verifiable parental consent and otherwise complying with COPPA have, on the one hand, discouraged site and service operators from allowing children on their sites or offering child-oriented content, and, on the other hand, raised costs for child-oriented sites. The average cost of compliance may well have fallen from the estimate provided to the FTC in 2005 ($45/child),[60] but even substantially lower costs on the order of $5-10 per child could represent a significant barrier to entry by sites that must rely, as most online sites and services do, on advertising revenues of scarcely more than that—and profit margins far less than that—per user per year. We must be realistic about these costs and the trade-offs involved in regulation. At some point, raising the cost of age verification for sites is simply no longer worth the marginal benefit to enhanced parental involvement and, indirectly, online child privacy and safety, because these values must compete with other values of parents and children, such as the competitiveness, creativity,

---

[58] Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (National Academy Press, 2002) at 224, www.nap.edu/openbook.php?isbn=0309082749&page=224.

[59] *See COPPA 2.0, supra* note 2 at 11.

[60] *See* Comments of Parry Aftab, *Request for Public Comment on the Implementation of COPPA and COPPA Rule's Sliding Scale Mechanism for Obtaining Verifiable Parental Consent Before Collecting Personal Information from Children* at 2, June 27, 2005, www.ftc.gov/os/comments/COPPArulereview/516296-00021.pdf

innovation and diversity in media and tools available to children online. COPPA in its current form probably strikes a reasonable balance, but as noted above, there may indeed be things that the FTC can do to lower the costs of compliance for operators, thus allowing us to achieve COPPA's goals at a lower cost to kids and parents in foregone content and services. I am also pleased that the Implementation Review asks about the need to update the "sliding scale" of parental consent verification methods and to offer greater flexibility to site operators, as noted above.

But I do worry that the Commission has explicitly invited proposals for legislative changes to the statute itself. Two questions from the Review are particularly troubling:

> **6**. Do the definitions set forth in Part 312.2 of the Rule accomplish COPPA's goal of protecting children's online privacy and safety? …
>
> **28**. Does the commenter propose any modifications to the Rule that may conflict with the statutory provisions of the COPPA Act? For any such proposed modification, does the commenter propose seeking legislative changes to the Act?

Note that question #6 does *not* include the critical limitation "consistent with the Act's requirements," which appears no less than 17 times in subsequent questions about specific aspects of the current rules. Whatever the FTC intended by this omission, when combined with question #28, it will be taken as an open invitation by many commenters to propose not just changes in how the COPPA rules are implemented, but wholesale revisions to the COPPA statute itself.

Ultimately, it is the responsibility of Congress, not the FTC, to make decisions about modifying the statute. If Congress wants an agency to spend taxpayer resources evaluating whether a substantial change to the agency's statutory authority is warranted, Congress is perfectly capable of authorizing, and appropriating funds for, such an inquiry. This is precisely what Congress recently did in the Child Safe Viewing Act, when it specifically asked the Federal Communications Commission (FCC) to prepare a report on online child safety issues.[61] Similarly, the Recovery Act of 2009 charged the FCC with preparing a national broadband plan.[62] Or, where less substantial statutory changes are at issue, the congressional committee with jurisdiction could request that an agency prepare a report to advise that committee. But as a general matter, regulatory agencies should not be in the business of reassessing the adequacy of their own powers, since the natural impulse of all bureaucracy is to grow, and it is through our elected representatives in Congress, not regulatory agencies—even those with the

---

[61] Child Safe Viewing Act, S. 602, 110th Cong. (2007).

[62] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (codified at 47 U.S.C. § 1305) ("2009 Recovery Act"); *see also*, *A National Broadband Plan for Our Future*, GN Docket No. 09-51, Notice of Inquiry, 24 FCC Rcd. 4342 (2009) ("*NOI*").

best of intentions—that "We People" are ultimately represented in deciding how to regulate the online (and offline) world.[63]

Finally I was surprised not to find a single mention of the word "education" in the FTC's Implementation Review Request for Comments. As explained above, just about everyone involved in debates about online child safety and privacy would agree that the solution begins with education—even if it doesn't end there. One might have thought the FTC would ask about whether effective implementation of COPPA's goals required more education efforts rather than (or perhaps in combination with) "stronger" regulations. Again, a layered approach of education, empowerment and enforcement is the best way to enhance the privacy and safety of children online, but education is truly the key.

Related PFF Publications

- *Written Testimony to the Senate Committee on Commerce, Science & Transportation's Subcommittee on Consumer Protection on "An Examination of Children's Privacy: New Technologies & the Children's Online Privacy Protection Act"*, April 29, 2010.
- *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, Berin Szoka & Adam Thierer, Progress on Point 16.11, May 2009.
- *Written to Maine Legislature on Act to Protect Minors from Pharmaceutical Marketing Practices, LD 1677*, Berin Szoka, March 4, 2010.
- *Parental Controls & Online Child Protection: A Survey of Tools & Methods,* Adam Thierer, Special Report, Version 4.0, Fall 2008.
- *Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation Are the Answer*, Adam Thierer, Progress on Point 16.13, July 8, 2009.
- *The Perils of Mandatory Parental Controls and Restrictive Defaults*, Adam Thierer, Progress on Point 15.4, April 11, 2008.
- *Written Testimony to House Committee on the Judiciary on Cyber Bullying and other Online Safety Issues for Children*, Berin Szoka & Adam Thierer, Sept. 30, 2009.
- *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, Comments of Berin Szoka to FTC Exploring Privacy Roundtable, Nov. 2009.
- *Privacy Polls v. Real-World Trade-Offs*, Berin Szoka, Progress Snapshot 5.10, Oct. 2009.
- *Online Advertising & User Privacy: Principles to Guide the Debate*, Berin Szoka & Adam Thierer, Progress Snapshot 4.19, Sept. 2008.
- *Targeted Online Advertising: What's the Harm & Where Are We Heading?*, Berin Szoka & Adam Thierer, Progress on Point 16.2, April 2009.
- *How Financial Overhaul Could Put the FTC on Steroids & Transform Internet Regulation Overnight*, Berin Szoka, Progress Snapshot 6.7, March 2010.

---

[63] *See, e.g., Super-Sizing the FTC & What It Means for the Internet, Media & Advertising*, PFF Briefing, at 22-23, April 16, www.pff.org/issues-pubs/pops/2010/pop17.6-transcript.pdf.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
202-289-8928 ■ mail@pff.org ■ @ProgressFreedom ■ www.pff.org