TECH FREEDOM

Comments of
Berin Szoka, President
TechFreedom[1]

on
Proposed Modifications to the
Children's Online Privacy Protection Act (COPPA)

Before the Federal Trade Commission[2]
September 24, 2012

Any conversation about revising the COPPA Rule should begin by recalling the original goals of the COPPA statute, expressed by the Act's Congressional sponsors:

> (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.[3]

Applying COPPA more strictly can actually frustrate these goals because, if children under thirteen cannot access the content and services they want, they will simply lie about their age—often with their parents' encouragement. Research published last year by Danah Boyd and others concluded that:

1. Parents and youth believe that age requirements are designed to protect their safety, rather than their privacy.
2. Parents want their children to have access to social media service to communicate with extended family members.
3. Parents teach children to lie about their age to circumvent age limitations.
4. Parents believe that age restrictions take away their parental choice.[4]

---

[1] Berin Szoka is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on COPPA. In particular, he previously submitted comments on the COPPA Rule Review on December 23, 2011, available at http://tch.fm/OmLmAz ("Szoka Comment") testified on COPPA before the Senate Commerce Committee on April 29, 2010, available at http://tch.fm/syexUo, ("Szoka Testimony") and is the author, with Adam Thierer, of *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech* (June 2009) ("COPPA 2.0"), available at http://tch.fm/rAhJbf.

[2] COPPA Rule Review 16 CFR Part 312, Project No. P104503 ("Supplemental NPRM").

[3] 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

[4] Danah Boyd, How COPPA Fails Parents, Educators, Youth (June 2010), http://www.zephoria.org/thoughts/archives/2010/06/10/how-coppa-fails-parents-educators-youth.html (previewing research published later, Danah Boyd, Eszter Hargittai, Jason Schultz & John Palfrey, *Why Parents*

These are the unavoidable consequences of COPPA's application only children and to sites and services that either have "actual knowledge" they are collecting personal information from children, or that are "directed to" children. This limited scope is not just a limitation of the COPPA statute—something Congress could change at a whim—but a requirement of the First Amendment. The Supreme Court has ruled that the government may not require operators of web sites and online services to treat their adult users like children simply because some may, in fact, be children.[5]

It was chiefly for this reason that, when the agency issued its first NPRM on the COPPA rule revision, we gave the FTC credit for rejecting calls to ask Congress to raise the age ceiling of COPPA—which would have raised the same constitutional problems as the unconstitutional Child Online Protection Act (COPA).[6] Here, the FTC deserves credit for recognizing:

1. That "many children may choose to lie about their age,"[7] the inevitable consequence of COPPA not covering sites that appeal to both children and adults;
2. That COPPA will not protect anyone, and will actually frustrate—rather than enhance, as Congress intended—parental involvement in children's online activities, if the law discourages operators from offering sites and services that will be covered by COPPA or if COPPA renders the sign-up for those sites and services too cumbersome or too expensive.

These are the constitutional and practical constraints within which COPPA must operate, and which must limit the FTC's ambitions. Given these constraints, the best we can do is to create a COPPA regime in which site operators are encouraged not only to offer specifically designed sites and services to children under 13 but, even better, to build sites and services that can "scale up" by offering "junior" versions that parents can manage, but with "training wheels" that come off as kids get older. Only if children actually want to use these sites will they—and their parents—cease lying about their age. This is no different from the problem of protecting copyright online: copyright-holders' best weapon against piracy is offering easily accessible versions of their content that consumers actually want to use.

I. Summary of Responses to the FTC's Proposed Changes to the COPPA Rule

The FTC's proposed revisions to will greatly expand the number of entities subject to the COPPA rules ("Rules"). Unfortunately, and despite the FTC's best intentions, this will likely reduce the number of sites and services available to children, as well as their profitability, and thus their quality—and thus, ironically, encourage children to lie to circumvent COPPA. Some of the

---

Help Their Children Lie to Facebook About Age: Unintended Consequences of the 'Children's Online Privacy Protection Act'", First Monday (Nov. 2011), http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075

5 *See* Ashcroft v. ACLU, 535 U.S. 564 (2002). *See generally*, Szoka & Thierer, *COPPA 2.0*, *supra* note 1.

6 Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59805 (Sep. 27, 2011) ("[T]he Commission does not recommend that Congress expand COPPA to cover teenagers.").

7 Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643, 46646 (Aug. 6, 2012).

proposed changes raise questions of the FTC's statutory authority in promulgating these definitions, threatening the rule of law the Internet marketplace relies upon.

If COPPA is to fulfill its original goals, the FTC must carefully consider the unintended consequences of revising COPPA's key terms. In particular, the FTC should:

1. **Clarify** that, for a website to be "directed to" based on **demographic evidence**, either a majority of audience must be children and, if it must go further, specify a lower threshold above which a site would be considered "directed to children" unless it asks users for their age before collecting information from them.
2. **Retain** the existing actual knowledge and "directed to" standard, rather than establishing a new "**reason to know**" standard in the definition for web sites and online services "directed to" children.
3. **Clarify** that **persistent identifiers** which do not permit contact with individuals and are not associated with personal identifiers are not personal information under the rule.
4. **Clarify** that its proposed joint liability for the use of plug-ins does not apply to third party content embedded by users on COPPA-covered sites.
5. **Clarify** that the "collected or maintained on behalf of an operator" proviso added to the definition of operator does not apply to plug-in operators that do not exchange personal information with the operators of COPPA sites.
6. Consider holding a **public workshop** on how these changes will affect the ability of site and service operators to offer versions of their products that children will actually *want* to use.
7. Explain whether companies have to get **re-permission from existing users for information** collected in the past now considered personal.

II. The Definition of "Web site or online service directed to children"

The FTC's intentions in revising the Definition of "Web site or online service directed to children" are admirable. The first proposed change—clarifying that the "totality of the circumstances" suggest that the site or service, "is likely to attract children under age 13 as its *primary audience*"[8]—is eminently reasonable, and will help to avoid uncertainty among site operators who might fear their site could be covered by COPPA. Such uncertainty could, on the margin, drive site operators not to offer content geared towards teenagers, for fear that it might bring them under COPPA. However, the FTC should clarify what, precisely, it means by "primary," which could be interpreted to mean either plurality or majority. Since it is unclear what the plurality would (presumably relative to other the age cohorts into which demographics are commonly divided) and there is no principled dividing line, and to avoid the problems described immediately below, the FTC should clarify that, by "plurality," it means "majority."

[8] *Id.*

The second proposed change is more problematic—and less easily fixed. The FTC has never before 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." The FTC now proposes that, in cases where "totality of the circumstances" test suggests that the site or service "is likely to attract an audience that includes a disproportionately large percentage of children under age 13 as compared to the percentage of such children in the general population," the site or service will be covered by COPPA unless it "(i) Does not collect personal information from any visitor prior to collecting age information; and (ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first obtaining verifiable parental consent."[9] This would, as the FTC notes, create gradations along the "child-directed" continuum, which is a good thing in principle.

But this revision may not achieve its intended aim. Operators with relatively high percentages of users under thirteen will simply put up ineffective age gates, which children will lie to get around—again, often with their parents' encouragement. The greater the burden of COPPA compliance, the more likely operators will be to do so. The essential problem here is a constitutional one: such age-gates *might* be relatively effective *if* they could require some credential to verify the age of the user, such as a credit card (hardly a foolproof method of verification but more effective than simply asking users for their age)—and yet, the Supreme Court has foreclosed that path because it infringes on the First Amendment rights of adult users to use the Internet anonymously, and of site operators to speak to such willing listeners. Thus, the conundrum of COPPA: the law cannot constitutionally mandate effective age verification, and so it will simply encourage under-13 users to lie.

It is particularly important to remember here that this requirement applies to "collection," a term which COPPA defined to include offering any functionality that allows children to communicate with other users, and thus potentially share personal information. Thus, this requirement would essentially fall on *all* social networking sites and burden the expression of users—not just the collection of information by sites.

It might be best for the FTC to drop this "disproportionately large percentage" provision altogether. But at a minimum, the FTC should specify just how high a percentage is enough. If, indeed, "plurality" means majority, the FTC presumably would want this threshold to be relatively lower—so as to encourage sites with a high percentage of users under 13 to at least request their users' ages, however ineffectual that might be. There is no principled way to draw this line; it is simply an exercise in prudence. But drawing *some* line is better than drawing no line. Given that 20% of the U.S. population is under 14 (the Census Bureau does not break down demographics under 13),[10] one option might be to draw the line at 150% of that level: 30%. This line, while as arbitrary as any other, would at least ensure that the

---

[9] *Id.*

[10] United States Census Bureau, Age and Sex Composition: 2010 (2010) at 4, *available at* http://www.census.gov/prod/cen2010/briefs/c2010br-03.pdf.

requirement to request user ages not be imposed on too many sites. While such a requirement might not raise the same constitutional concerns as did the age-verification mandate under COPA (because requiring a credit card is far more privacy-invasive and likely to chill speech than simply asking for a user's age), a requirement to impose a simple age-gate *does* still implicate some of the same values: COPPA should not burden adult users and require altering the Web.

III. The FTC Risks Exceeding Its Statutory Authority

Among COPPA's chief virtues has been that the FTC's definitions under COPPA have never triggered a legal challenge—unlike the law's two precursors, the Communications Decency Act of 1996 and the Child Online Protection Act (COPA) of 1998, both of which were ultimately ruled unconstitutional.[11] Yet, in proposing to revise the COPPA Rule's definitions of "web site or online service directed to children" and "personal information", the Commission risks exceeding its statutory authority under COPPA statute (the "Act"),[12] which requires that:

1. The term "personal information" may be re-defined as technology changes, but only to include those pieces of information that permit direct contacting of a child or include persistent identifiers which are associated with individually identifiable information.
2. An operator who is not directing its content to children must have actual knowledge in order to be subject to the COPPA Rule.

Both issues are considered below.

A. Does the FTC have the authority to modify the definition of "personal information" to include persistent identifiers which are not associated with individually identifiable information under the COPPA statute?

Under the COPPA statute, the FTC has an important—but limited—authority to redefine the scope of personal information. This personal information must be (1) individually identifiable information (2) collected online that (3) the Commission determines "permits the physical or online contacting of a specific individual"—or other information associated with such identifier.[13] Under this authority, the FTC offered the following proposed revision:

---

[11] *See* Reno v. ACLU, 521 U.S. 844 (1997) (striking down the CDA). 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. *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-stillunconstitutional.

[12] *See, e.g.*, Chevron USA Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837, 842-43 (1984) ("When a court reviews an agency's construction of the statute which it administer. . . the question [is] whether Congress has directly spoken to the precise question at issue. If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress.").

[13] 15 U.S.C. § 6501(8)(F) ("The term 'personal information' means individually identifiable information about an individual collected online, including— any other identifier that the Commission determines permits the physical or online contacting of a specific individual.").

> "*Personal information* means individually identifiable information about an individual collected online, including:
>
> > (g) A persistent identifier that can be used to recognize a user over time, or across different Web sites or online services, where such persistent identifier is used for functions other than or in addition to support for the internal operations of the Web site or online service. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."[14]

The FTC has the authority to determine whether an identifier permits the physical or online contacting of a *specific* individual. This authority is limited by the Act, though, which only allows the FTC to extend the definition of personal information to individually identifiable information. Many persistent identifiers—such as cookies, IP addresses, and unique device identifiers—do not allow web sites or online services to identify *specific* individuals. Insofar as this rule applies to such instances, it is inconsistent with the unambiguous intent of Congress as evinced in the statute.

Previously, the FTC recognized the distinction between persistent identifiers and personal information, and treated these differences under the statute accordingly:

> One commenter asked the Commission to clarify that operators are not required to provide parental notice or seek parental consent for collection of non-individually identifiable information that is not and will not be associated with an identifier. **The Commission believes that this is clear in both the Act and the Rule.** [...]
>
> One commenter noted that there are some persistent identifiers that are automatically collected by websites and can be considered individually identifying information, such as a static IP address or processor serial number. [...] **The Commission believes that unless such identifiers are associated with other individually identifiable personal information, they would not fall within the Rule's definition of "personal information."**
>
> Several commenters asked whether information stored in cookies falls within the definition of personal information. **If the operator either collects individually identifiable information using the cookie or collects non-individually identifiable information using the cookie that is combined with an identifier, then the information constitutes "personal information" under the Rule, regardless of where it is stored.**[15]

---

[14] Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643, 46647 (Aug. 6, 2012).

[15] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 59892 (Nov. 3, 1999).

The FTC's proposed revision invites litigation that could tie up the revision of the Rules. To avoid such an outcome, and the uncertainty even the specter of litigation would create, the FTC could clarify that persistent identifiers qualify as personal information under COPPA only when associated with other individually identifiable information covered by COPPA—as I suggested in the 2010 white paper "COPPA 2.0," I co-authored with Adam Thierer.[16]

B. Does FTC have authority to set up "reason to know" standard under the Act?

The Act clearly states that: "It is unlawful for an operator of a website or online service directed to children, or any operator that has *actual knowledge* that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b) of this section."[17] Yet the FTC's proposed COPPA revision will apply to operators who both "know or [have] reason to know that it is collecting personal information [from children under 13]."[18]

To the extent that this proposed standard differs from the "directed to" standard in the statute, it exceeds the FTC's statutory authority. In other words, the COPPA statute already includes a constructive knowledge standard, but one in which constructive knowledge is inferred from objective criteria about the content itself—namely, the nature of the content of the site (e.g., its use of cartoons or terminology geared towards kids). By contrast, the FTC's proposed revision would create a constructive knowledge standard in which knowledge could be inferred from a wide range of other factors—essentially creating a *de facto* "notice and take down regime." The problem with such regimes, in general, is that they create a perverse incentive for online operators to simply take down content upon receiving notice, without any real inquiry into the circumstances because such inquiries do not scale—or not to offer the functionality that creates the potential liability in the first place. Here, many sites may simply choose to cripple functionality that allows users to share content (which COPPA considers "collection").

Interestingly, the FTC previously recognized the pitfalls of such constructive knowledge tests in the earlier stage of this rule review.[19] There the FTC determined it was best to retain an actual knowledge standard.[20] Now, the FTC has decided this lesser standard is necessary in order to

---

16 Szoka & Thierer, *COPPA 2.0*, *supra* note 1, at 10 ("COPPA would consider collection to occur through the use of persistent identifiers such as cookies 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.")

17 15 USC § 6502(a)(1) (emphasis added).

18 Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643, 46645 (Aug. 6, 2012).

19 Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59806-07 (Sep. 27, 2011) ("[I]mposing a lesser 'reasonable efforts' or 'constructive knowledge' standard might require operators to ferret through a host of circumstantial information to determine who may or may not be a child. . . Were the Commission to recommend that Congress change COPPA's actual knowledge standard, the changes the Commission proposes to the Rule's definitions *might prove infeasible* if applied across the entire Internet.") (emphasis added).

20 *Id.* ("Despite the limitations of the actual knowledge standard, the Commission is persuaded that this remains the correct standard to be applied to operators of Web sites and online services that are not directed to

ensure cooperation between different operators. In the Supplemental NPRM, the FTC explains that the phrase "'reason to know' does not impose a duty to ascertain unknown facts, but does require a person to draw a reasonable inference from information he does have."[21] Nonetheless, it's unclear what it means for the online company to have the information. Would an email to a mid-level executive or posting on a social media site run by the organization be enough? Such concerns are magnified by the FTC's recent imposition of a record $22.5 million fine on Google for a statement made in an online help file that became untrue only because a rival changed how its technology worked—another variant of a constructive knowledge standard, that was not explained in the FTC's consent decree.[22]

The FTC should reconsider this re-definition to avoid possible statutory conflicts that could tie up this rule revision in litigation and create uncertainty in the marketplace for children's sites and services.

IV. Imposing Intermediary Liability Would Ultimately Hurt Children

The FTC's proposed revision of "operator," when combined with its redefinition of "web site or online service directed to children" would, together, impose liability on a number of third party plug-in developers, creating a cloud of uncertainty. Imposing liability on intermediaries runs contrary to a general presumption in U.S. law that online intermediaries are not responsible for the actions of third parties.[23] Sec. 230 of the Telecommunications Act[24] has served the Internet well by immunizing providers and users of an interactive computer service from liability for publishing information created by others. While the FTC's goal is clearly to extend the Rule to cover more entities,[25] the far-reaching impact of this new definition will likely have unintended consequences for the vitality of children's content—just as intermediary liability always does.

The FTC should clarify that its proposed revision to the definition of "operator" covers only plug-ins that (i) the operator of a site or service actually installs on the site or service and (ii) the plug-in operator supplies identifiers collected through that plug-in to the operator in a way that would otherwise be covered by COPPA, or vice versa. The first clarification is important because, while this is what the FTC *seems* to contemplate when it refers to "an operator of a child-directed site or service that chooses to integrate into its site or service other services that

---

children. Accordingly, the Commission does not advocate that Congress amend the COPPA statute's actual knowledge requirement at this time.").

21 Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643, 46645 n.18 (Aug. 6, 2012).

22 FTC Press Release, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012) http://www.ftc.gov/opa/2012/08/google.shtm.

23 *See* 47 U.S.C. § 230.

24 47 U.S.C. § 230.

25 Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643, 46649 (Aug. 6, 2012) ("The Commission staff is unaware of any empirical evidence concerning the number of operators subject to the Rule. However, based on the public comments received and the modifications proposed here, the Commission staff estimates that approximately 500 additional operators may newly be subject to the Rule's requirements and that there will be approximately 125 new operators per year for a prospective three-year period.").

collect personal information from its visitors,"[26] the actual definition leaves open the possibility that simply allowing users to embed content from third party services qualifies as "integration" into the site. For example, some bulletin boards bar embeds of third party content (if only to prevent newly registered members from spamming other members). This is certainly something child-directed sites *could* do, but it might impoverish the experience of their users if they could not, for example, embed content from third party platforms like YouTube in the way that users can on the rest of the Internet—a potential reason to lie to get access to more functional sites, for example. And what good would it do? Why do we care if third parties can collect information about activity using their plug-ins by children on COPPA sites—provided the plug-in operator is not sharing information with the site operator?

More fundamentally, what really *is* the difference between the user embedding a piece of third party content (which will generally include a tracking element for analytics purposes, if nothing else) and the site doing so—if the site is not receiving information from the third party?

From the third-party plug-in operator's perspective, the problem is that such operators make their plug-ins available to anyone to install or embed on their own site—without knowing who is using them. If plug-in operators are held jointly liable for data collection under COPPA, many will simply ask whether the operator intends to use their plug-in on a site directed to children or whether the operator has actual knowledge that the site collects information from children—just as many adult-oriented sites today simply ask users to certify that they are not under 13. In one respect, this system would work better, since the operators of COPPA-covered sites and services will not simply lie on a massive scale to get access to plug-ins, as children lie to get access to content. Instead, the problem is that such a rule *could* be effective—but the effect would simply be to deny such sites plug-in functionality. How does that benefit children-directed sites? Does it, rather, simply make them less competitive with the sites that appeal to a slightly older age group—which are just one lie away?

Of course, it may make sense to hold third parties liable if they set up a relationship to exchange data with the children-directed site or service, whether informally or by contract, provided they know that the plug-in would be used in this way. (And, of course, such plug-ins are already covered by COPPA if they are of such a nature as to be evidently "directed" to children, just as any site would be—such as if the plug-in features cartoon characters.) But, the proposed definition of "Operator" goes much further, treating all plug-ins as having a pre-existing relationship with the children-directed web site or service. This would create a great deal of regulatory uncertainty for plug-in developers, who may no longer allow their plug-ins to be used at all by sites or services unless it can be verified the site or service is not targeted at children.

For instance, plug-ins like the Facebook "Like" button or Google's "+1" button are often placed on web sites and online services which children may be interested in. If one of these websites has knowledge that a child is under 13 but for some reason the child has an account with either

[26] *Id.* at 46644.

Facebook or Google (and is thus able to use one of those plug-ins), what are the website's responsibilities? Under the new definition of Operator, it appears that the first party website would be subject to intermediary liability for the actions of the third party plug-in.

V. Restricting Advertising Will Impoverish Children's Sites & Services, Encourage Lying

The FTC deserves credit for recognizing the importance of advertising to fund children's media by including within the "Internal Operations" exception to the definition of personal information the use of information to "serve contextual advertising on the Web site or online service."[27] But this exception may prove inadequate for child-directed sites that are dependent on advertising. To start with, the essential point about online advertising is that it is *not* an "internal" operation; rather, the vast majority of sites, particularly smaller sites, rely on third parties to place ads—through what are essentially plug-ins embedded on the site. (Requiring COPPA-covered sites to handle advertising directly would be economically devastating.) In the case of both content plug-ins and ad plug-ins, the plug-in collects data to "track" the user across sites. The only essential differences are:

1. The ad network has a financial, contractual relationship with the site operator.
2. The third party (the ad network) uses the data to display relevant advertising (not just for analytics, etc.).

The first difference does give the ad network the opportunity to ask its partners whether their sites are directed at children. But why should ad networks be held responsible if a COPPA-covered site falsely states that it is not COPPA covered—or if a site finds itself covered by COPPA but genuinely thought it was not when it signed up for advertising? With hundreds of thousands of publishers in the Google Display Network,[28] for example, it is simply impractical for even a large company like Google to predict whether a site will be covered by COPPA. Imposing such intermediary liability will simply cause Google to drop advertisers that *might* be COPPA covered—just as User-Generated Content site operators respond to DMCA take-down requests by erring on the side of caution, taking down more content than legally necessary, or simply disabling UGC content altogether.

The second difference seems immaterial. What difference does it make whether the plug-in operator collects data for analytics or to show advertising? Restricting how many ads there are, or even how relevant the ads are, simply is not among COPPA's intended goals. Consider the case of retargeting, which is sometimes classified as "behavioral": If a child views a particular book on a booksellers' site, why should the ad network not be able to sell ads to the operator of the book site showing an ad for that book on other sites the child might visit? The key, from a statutory perspective, is that neither the bookseller site nor the ad network nor the operator of COPPA-covered site need have any idea who the child is—or any means of contacting a "specific individual" child. Such advertising may be distasteful to those who simply do not like advertising, but it can be an essential revenue source for the publishers of ad-supported sites—

---

[27] *Id.* at 46648.

[28] http://support.google.com/adplanner/bin/answer.py?hl=en&answer=96261

and thus confer enormous, if indirect, benefits on children. Why is COPPA any more implicated in this example than if the bookseller simply placed ads on the same sites on a much less targeted basis based on general assumptions about the overall demographics of these sites? Simply put, COPPA does not require inefficiency.

The better way to handle this issue would be to take the same approach to advertising data as to information collected through plug-ins—*i.e.*, to apply COPPA whenever (i) the ad network exchanges identifiers with the site operator as would otherwise be covered by COPPA, such as by enriching user profiles held by either party with behavioral data, or (ii) where the ad network itself would be covered by COPPA.

If, however, the FTC retains its existing definition, it should clarify that third-party ad networks are included in the definition of "internal uses" (despite the natural reading of that word). The FTC should further clarify that the list of exceptions should be considered illustrative and not exclusive—to ensure that the exception captures all data practices necessary to successfully engage in advertising that does not result in the collection of truly personally identifying information.

Ultimately, the FTC's attempt to restrict behavioral advertising without limiting contextual advertising is an attempt not to limit what information is collected but how it is used—since the essentially the data sets will be collected for both purposes. It is worth remembering that the Digital Advertising Alliance's voluntary code already prohibits its members from engaging in behavioral targeting "directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA."[29] Why does COPPA need to do more?

Ultimately, the less money available to children's sites, the less useful and attractive to children they will be—and the more children will simply lie to gain access to better-funded sites. Thus, attempting to restrict profitable forms of advertising that do not engage in the creation of "digital dossiers" tied to any true identifiers covered by COPPA (name, address, social security number, photo, *etc*.) could be highly counter-productive even under COPPA's direct goals, while also harming the vibrancy of the ecosystem for children's media.

Given the vital importance of this subject, the FTC should consider holding a workshop on the value of advertising in children's media and whether this value will be adversely affected by the proposed rules.

VI. Proposed Changes Should Not Be Retroactive

The FTC's changes to the definitions of "personal information," "directed to," and "operator" all raise a critical question the FTC's FNPRM does not answer: Will these changes be applied retroactively? In other words, what should companies do about (i) previously collected data which is now considered personal information or (ii) personal information they gathered in the past before they were considered operators covered by COPPA. Whether or not the FTC

[29] Digital Advertising Alliance, Self-Regulatory Principles for Online Behavioral Advertising at 17 (July 2009), http://www.iab.net/media/file/ven-principles-07-01-09.pdf

ultimately determines the rules should have retroactive application, if this question is left unresolved in the FTC's rulemaking, the perceived risk of enforcement action could lead companies to have to obtain parental consent for this information, or, if their audience includes older users (such as would be the case under the FTC's proposed revisions to "directed to"), to age-verify the users with whom the data is associated to determine their ages.

This, ironically, would result in the collection of *more* data, either about users' ages or to verify the parent-child relationship or to get a credit card on file. Or, it could result in the deletion of previously collected personal information. While the latter prospect may delight those who believe that data is inherently dangerous and thus that all data minimization is necessarily good, the data in question would include not only personal data collected by websites in profiles for advertising or analytics purposes, but also communications by users—because, again, the term "collect" under COPPA includes enabling users to share personal information. Thus, for example, if a site or service fears it will be covered by COPPA for the first time, it may simply delete user-generated content such as message board postings—and block such sharing in the future. This could raise serious constitutional problems such as implicated in the COPA case.

VII. Conclusion: Consider the Values at Stake, Reconsider the Hard Questions

We must not lose sight of the forest for the trees. Any revision of COPPA should consider not only the stated goals of COPPA's congressional sponsors, but also the following values —as we suggested in our earlier comments on the COPPA Rule Review.[31]

1. **COPPA-Covered Sites Must be Attractive**. If COPPA-covered sites cannot compete with general audience sites because their functionality is limited, or their funding is too limited to support free offerings, or if they must charge for access, children and parents will simply lie about their age to access better sites.
2. **Power & Simplicity of Parental Control**. Parents should have the opportunity, and means, to decide how much sharing of personal information based on their own values and judgments about privacy, safety and exposure to marketing. This control should scale with the childhood development states. Ideally, parents should be able to tailor their children's experience beyond making binary decisions about whether to authorize a site or service.
3. **Privacy & Security**. While it might seem obvious that COPPA should enhance, rather than undermine children's privacy and the security of data collected about children, COPPA could, if revised imprudently, result in the collection of *more* data about children, and increase the risk of exposing that data to those who might mis-use it.
4. **Education & Citizenship.** Digital media should offer children a vehicle for developing as informed citizens of an information society and economy. Using sites and services

[31] *See* Szoka Comment, *supra* note 1, at 1-2.

appropriate for their developmental maturity ensures that they will be well-prepared later on in life, and that our educational system can make effective use of digital tools.

5. **Expression**. Digital media should empower children to express themselves, subject to parental control. Remember, COPPA covers expression by users, not just "tracking" by sites.
6. **Abundance**. Digital media should be abundant, much like the broader Internet.
7. **Diversity**. Digital media should be diverse, much like the broader Internet.
8. **Affordability**. Digital media should cost as little as possible without compromising quality.
9. **Innovation**. Digital media should, like the rest of the web, constantly improve in quality, sophistication, and interactivity.
10. **Competition**. Competition in digital media and low barriers to entry will promote abundance, affordability and innovation.

Ultimately, the FTC should look for every opportunity it can to promote the development of services children will actually want to use. The FTC should also consider holding a workshop on how sites and services can serve the under thirteen market. In addition to the questions raised above, this workshop should consider what changes may be necessary to the rules or, indeed, to the statute itself, to allow general audience sites and services to offer "junior" versions of their services appropriate for children and compliant with COPPA.

If anything, this will require not the imposition of intermediary liability but the opposite—ensuring that app social networking platform operators like Facebook, and app store operators like Microsoft, Apple and Facebook (and potentially broadband and gaming companies and other companies yet to be conceived) are able to serve as clearinghouses to process parental consent for apps made available to children. If, instead, these intermediaries are liable for the failure of apps to fully comply with COPPA, the practical result will be that no market will develop for under-13 apps that parents can control and customize to meet their children's needs. This will only encourage more lying—and the prolong fiction that children (and their parents) will remain content with the limited offerings currently available to them.

The FTC began this inquiry "on an accelerated schedule," as it acknowledged when releasing the initial NPRM.[32] Why rush the resolution of these complicated questions? The agency has plenty of time to consider these changes to COPPA carefully—including holding another public workshop.

---

[32] FTC, Press Release, "FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule," (Sept. 15, 2011) http://www.ftc.gov/opa/2011/09/coppa.shtm