Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In the Matter of	)	
	)	
COPPA Rule	)	Docket No. 339
Review	)	Project No.P104503

COMMENTS OF CENTER FOR DEMOCRACY & TECHNOLOGY and AMERICAN LIBRARY ASSOCIATION

The Center for Democracy & Technology (CDT) and American Library Association (ALA) respectfully submit these comments in response to the Commission's August 2012 proposed revisions to the Noticed of Proposed Rulemaking of the COPPA Rule, originally issued in September 2011.[1]

Introduction

Commenters support the Commission's decision to update COPPA to address evolving data collection practices on the internet. Today's websites increasingly incorporate third-party content from a diverse range of services, which in turn have the ability to generate detailed profiles about user's online behavior (including under-13 users, many of which have lived with the internet all their lives). For these reasons, we believe it is reasonable to expand the definitions of "operator" and "personal information" in the COPPA Rule to reflect the modern online ecosystem. However, Commenters are very concerned that the Commission's most recent proposals may move the COPPA Rule toward a constructive knowledge standard, which would impose massive burdens on general-purpose websites and widgets and would upset the delicate balance between children's privacy and all users' free expression rights that was achieved in the original COPPA statute and Rule. We agree that more should be done to stop unwanted behavioral advertising to children, but the proposed Rule significantly overreaches and raises real concerns for free expression and innovation in online services for children, older minors, and adults. We believe that the Commission's proposed regulatory language must be refined to comport with COPPA's traditional narrow scope focusing on operators with actual knowledge or who intentionally direct their sites or services primarily to children.

I. Operators of Third-Party Plugins Should Not Have Independent COPPA Obligations Unless the Plugins Are Directed to Children or the Operators Have Actual Knowledge that They Are Collecting a Child's Personal Information.

[1] Federal Trade Commission, Children's Online Privacy Protection Rule, Proposed Rule, 76 Fed. Reg. 187, 59805 (Sep. 27, 2011)(hereinafter "Proposed Rule"), *available at* http://ftc.gov/os/2011/09/110915coppa.pdf.

Commenters support the Commission's expansion of the term "operator" to reflect that third party services may well collect and process children's personal information through sites directed to children, and that it is appropriate to require first-party sites to disclose and obtain consent for the information collection they choose to enable.[2] However, the Commission should clarify that the third parties themselves do not have independent COPPA obligations unless the third party's content is *directed to children* or the operator has *actual knowledge* that it is collecting personal information from a child. The proposed expansion of COPPA's scope to an operator of a plugin that "knows or has reason to know" its plugin is being used on a children-oriented site[3] is unduly vague and sets up a potentially burdensome and unreliable notice-and-takedown regime that would not substantially advance children's privacy. For widgets and other embedded third party content, the responsibility for complying with COPPA should fundamentally lie with first parties who have the direct relationship with users, except in the rare circumstances when a plugin purposefully targets children or has actual knowledge that it's collecting children's information.

A. COPPA Notice and Parental Consent Obligations Should Remain the Responsibility of Operators of Websites and Online Services that Are Themselves Directed to Children.

In CDT's 2011 comments to the Commission on the initial Proposed Rule, we stated that independent entities or third-party services should not have independent COPPA obligations based on the actions taken by first-party site operators. Most third-party widgets and content do not directly interact with users or have preexisting relationships with those users, and thus they will rarely obtain "actual knowledge" that they are collecting a child's personal information. Indeed, they often do not directly interact with the first-party operators themselves — instead they make themselves available to first parties to place on their sites through a public-facing application programming interface (or in the case of applications, a software development kit (SDK) to plug into their own code). For example, both Twitter and YouTube offer embeddable content that anyone with an account on their service can use to copy and paste code that will display small versions of their websites on the embedding site.[4] In terms of platforms, a prominent example is Google's AdMob mobile advertising framework which requires application developers to download their Google AdMobs Ads SDK and simply add a few lines of

---

[2] As CDT discussed in its December 2011 comments, the first-party operator is in the best position to interact with the parent and child, to know that she is operating a child-directed site, and to obtain and provide information about the data collection practices of the third parties she allows to collect information through her site, whether the operator herself collects personal information from children or not. Commenters reiterate the caveat that the first-party's obligation should be limited to accurate identification of third-parties and reasonable disclosure of their data collection and use practices. First-party operators should not face liability for the actions of third parties to the extent they vary from the third-party's disclosed practices. Comments of Center for Democracy & Technology 5, Dec. 23, 2011, (hereinafter CDT December 2011 Comments) *available at* http://www.ftc.gov/os/comments/copparulereview2011/00367-82392.pdf.

[3] Federal Trade Commission, Children's Online Privacy Protection Rule, Proposed Rules, 77 Fed. Reg. 151, 46643 (Aug. 6, 2012) (hereinafter "Supplemental Proposed Rule"), *available at* http://www.ftc.gov/os/2012/08/120801copparule.pdf.

[4] See: https://twitter.com/settings/widgets/new; http://support.google.com/youtube/bin/answer.py?hl=en&answer=171780 (last visited Sep. 21, 2012).

code that will then render a small banner advertisement at the bottom of the device's screen when the application is running.[5]

If the Commission's aim is to give parents control over the behavioral tracking and targeting of their children, that goal should be accomplished by placing requirements on the applications and websites that choose to embed tracking content. For that reason, Commenters generally support the expansion of the definition of the term operator, to the extent that it places responsibility for third-party collection with the first party operator that enables and benefits from such collection (though, it is unclear how this language applies to platforms, *see infra* Section II). Indeed, the Commission could consider expanding its language to clarify that first party operators must offer a separate choice to parents about whether they consent to third party tracking of their kids' behavior (distinct from consent to share information with the first party itself). Such a requirement would comport with the COPPA Rule's existing language stating that the provision of service cannot be made contingent upon the transfer of children's information to third parties.[6]

However, the expansion of the definition of personal information to include IP address and other unique identifiers means that every third-party service on a website or application is potentially collecting personal information about its users. (But see *infra* page 6, discussing the Commission's need to clarify that the "support for internal operations" exemption applies to third-party plugins' own internal operations.) With this in mind, we urge the Commission not to replace COPPA's traditional actual knowledge/directed to children test for covered operators with the "reason to know" standard proposed in the supplemental Proposed Rule. This broad expansion of COPPA's reach would impose significant compliance costs on general-purpose third-party services that are not well-positioned to understand the audience they may be reaching, which will chill innovation in online services with limited benefit to children's privacy.

Only in rare situations should a third-party widget be deemed to have obligations under COPPA. Most general-purpose third-party widgets or functionality (such as advertising networks and analytics providers) do not direct their services to children. However, if a third-party widget's content is consciously directed at children, it is reasonable to expect that company to comply with COPPA. For example, if an advertising network includes segments targeted at under-13 users, it is reasonable to require the network to follow COPPA's strictures in collecting, using, and retaining information from users targeted by those advertisements.

Similarly, if a third-party widget includes functionality for a user to input age information, or because of a previous first-party interaction with the user the operator knows the user is under 13 as the user is interacting with the widget (e.g., a publisher that age-screens visitors on its own site, also offers third party widgets for other sites to use, and can identify an individual user as he interacts with the widget), COPPA should govern the information that operator collects through its widget on other sites.

---

[5] See: Google AdMob Ads SDK, "Banners I", available at: https://developers.google.com/mobile-ads-sdk/docs/admob/fundamentals (last visited Sep. 21, 2012).

[6] 16 C.F.R. 312.5(a)(2) (2011) "An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties."

B. The Proposed "Knows or Has Reason to Know" Standard is Too Vague.

In the supplemental Proposed Rule, the Commission suggests broadening COPPA's traditional definitions to include services that "have reason to know" they are collecting information through a child-directed site. Despite the explanatory footnote stating that such a standard does not require a party to obtain "unknown facts," it seems equally unreasonably to hold a company strictly liable for all facts somehow in its possession. For example, in a well-known case in Italy, Google was deemed to have "reason to know" that someone had uploaded a privacy-invasive video to Google's YouTube service because user-generated comments on the site complained about the video. It is unclear when the Commission would determine that an operator had attained a "reason to know" – when a concerned parent makes a phone call to a customer service line, sends an email to a human resources officer, or uses an online comment form? If "reason to know" extends to all information in a large, multinational company's possession, companies would have to implement burdensome compliance programs to scour all databases and manual sources of information for clues that any of the first parties embedding its content is directed at children.

But even if the rule were revised to require a notice-and-action regime (similar to the Digital Millennium Copyright Act's notice-and-takedown system for alleged copyright violations), where complaints must be forwarded to a dedicated person, this would still pose significant compliance costs for companies, both to monitor and to comply with notices. This would be especially true for small advertising networks or widget makers whose code has been widely deployed but who do not have full-time staff to monitor complaints. Developers of plugins and other interactive or cross-site widgets and services, many of whom could not afford to implement the necessary compliance mechanisms, will likely be discouraged from continuing to create new and innovative services.

Moreover, as with the DMCA, companies would likely comply as a matter of course with take-down requests rather than investigate the merits, due to cost and liability concerns.[7] Because apparently any person or entity could provide information to the plugin operator about the child-directed nature of the site (unlike the DMCA where notices must be highly specific and come only from the affected rightsholder or her agent), there is even less assurance that "notices" would be legitimate, Rather, it makes far more sense to place the fundamental responsibility on the first party operator who directly interfaces with users, and who is best positioned to know whether it is directed at children or has actual knowledge that it is collecting information from a child – whether through its own code or third-party code running on its site.

Otherwise, the uncertainty of "triggers" here and subsequent fear of these consequences will prevent plugin services from interacting with first-party websites, hurting innovation and preventing the development of rich online resources for children. It will discourage plugins from allowing sites directed to children to use their services, and may discourage some plugins from operating at all. It is possible this standard could go so far as to

---

[7] See, e.g., CDT, Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech, September 2010, *available at* http://www.cdt.org/files/pdfs/copyright_takedowns.pdf; CDT, Comments to European Commission on Notice-and-Action, March 2012 (regarding need for circumstances under which operators receive notice to be tightly controlled and safeguarded against abuse, need for statement of standing to issue notices), *available at* https://www.cdt.org/comments/comments-european-commission-notice-and-action.

function as a notice-and-takedown standard. Plugins that cannot afford COPPA compliance or do not want the burden will not make their services available on sites directed to children.

II. The Commission Should Clarify that Platforms Do Not Have COPPA Compliance Obligations for the Services They Enable.

The Commission should also clarify the role of third-party platform providers with regards to applications or other services developed on top of those platforms or that use their application programming interfaces (APIs). Commenters urge the Commission to clarify that neutral intermediaries such as platforms should not be required to vet third parties using their platform, or to be required to obtain consent (or otherwise comply with COPPA) on any third-party application's behalf.

Platforms — such as mobile applications stores and social networking sites that allow third parties to build on their networks — are first parties in that users interact directly with them, and they may in fact take identifying information from users. Unlike the "widget" or plugin context discussed above, however, in which first-party publishers/operators make concerted decisions about which third parties to embed — and thus should bear the responsibility for the data those third parties collect — platforms allow users to directly connect with other first parties, and do not make the final decision about what content the user interacts with.

Under the Commission's proposed revisions, it is not clear when information collected by those applications is considered collected "on behalf" of the platform. Clearly, online platforms benefit from the applications that run on them (especially when a platform such as an app store charges customers to use third party applications). But even relatively closed platforms that voluntarily vet or remove applications for certain reasons should not be required by COPPA to monitor which applications may be directed to children. Essentially, platforms function in a way akin to user-generated content sites, operating as intermediaries that provide the opportunity for developers to create and upload applications and users to select the content of their choice.[8] Consistent with the protections afforded intermediaries by Section 230 of the Telecommunications Act, 47 USC § 230, we urge that the Commission make clear that the responsibility for COPPA compliance lies with the party directing its services to a child, not with the platform, operating system, browser, or hosting facility that allows the developer to obtain users' personal information. Certainly, in all multi-party scenarios, *some* party must be responsible for the various data collection practices that children are exposed too. In the platform context, the fundamental responsibility should lie with the application running on top of the platform that makes the decision to target children or knowingly collect their data.

On the other hand, for platforms that are willing to shoulder the responsibility, it may be reasonable to allow the third party applications to outsource COPPA compliance to the hosting platform if the platform allows for it, so long as the terms are made clear to the consenting adult. That is, a platform such as an application store could obtain consent from parents to share their children's information with the some or all of the applications that use the platform. If such a model were permitted, the Commission should ensure

[8] Of course, entities that run platforms or otherwise act as intermediaries can (and do) develop their own content/applications and must be treated as the responsible party when they do.

that platforms are required to offer robust *ex ante* controls limiting the sharing of children's data with certain applications or categories of application (or even prohibiting the platform from sharing children's information with *any* other party[9]) as well as notification provisions to allow parents to monitor and adjust permissions to sharing of their children's information over time. While many parents will not wish to delegate to a platform the authority to give third party applications the ability to collect personal information from their children, others may want to empower their kids to share and obtain information through certain applications without being forced to sign off on every interaction with a new web service. As long as the terms are clearly presented and the parent is given strong controls, Commenters have no objection to COPPA allowing for parents to give some form of persistent permission to the collection of their children's personal information to the applications on a particular platform.

III. An Expanded Definition of "Personal Information" Must Provide for Reasonable Operational Use of Pseudonymous Identifiers.

Commenters agree with the Commission that an expanded definition of personal information to include "IP address and other persistent identifiers" necessitates an exemption for certain reasonable operational collection and usage of those identifiers. Companies should be encouraged to create content for children under 13 that involves the usage and retention of minimal user data and thus does not trigger COPPA obligations, including obtaining verified parental consent. Children's games that only collect IP addresses and a children's social network that collects name, age, and email address should not have the same regulatory obligations under COPPA, and services should be incentivized to collect as little information from users as necessary. We do, however, agree with the Commission that behavioral targeting of children using unique identifiers should trigger COPPA compliance obligations.[10]

However, the scope of what activities are permitted under the new definition of "support for internal operations" is not entirely clear. The lens through which we (and likely many others) view the question of excepted operational uses is the "Do Not Track" debate. CDT has previously argued that even when a site receives a "Do Not Track" instruction from a user agent, a third-party service or "plugin" should still be able to use unique identifiers to perform basic functionality such as content delivery, site analytics, contextual advertising, identity transaction, and fraud prevention.[11] Those uses seem to be clearly envisioned in the revised FTC definitions, but the FTC should be explicitly clear that the "support for internal operations" exemption applies to each operator's own functioning, and not solely to the primary site operator.

The most contested operational uses of data in the "Do Not Track" context, however, have been "market research" and "product improvement," and it is unclear how those

---

[9] Such a requirement would be consistent with the COPPA Rule's existing language prohibiting companies from conditioning service on the sharing of children's data with other parties. 16 C.F.R. 312.5(a)(2), *supra* note 6.

[10] Proposed Rule, *supra* note 1 at 59812; Supplemental Proposed Rule, *supra* note 3 at 46647.

[11] CDT, What Does "Do Not Track" Mean? Apr. 2011, *available at* https://www.cdt.org/files/pdfs/20110447_DNT_v2.pdf; Erica Newland, CDT's Proposals re: Template for Parties and Business Uses, Apr. 7, 2012, *available at* http://lists.w3.org/Archives/Public/public-tracking/2012Apr/0078.html.

purposes fare under subsection (a) of the revised Rule ("maintain or analyze the functioning of the Web site or online service"). Commenters' best guess is that "product improvement" might be allowed, while market research would be prohibited, but neither case is clear. Alternatively, it may just be the case that only maintaining and debugging of existing functionality, or only data siloed to any individual party, is allowed as an "internal operations" exception under subsection (a). In the "Do Not Track" context, CDT has argued that broad purposes like "market research" and "product improvement" should not be used to justify data retention and the use of unique identifiers when a user has made the decision to transmit a "Do Not Track" signal. The threat models may be different for the collection and use of information from children under the age of 13, but in any event the Commission should clarify how its standard will apply to these common uses of data.

Further, the FTC should state clearly that the operational use exception applies both to first parties and third parties in any given context. We believe that this is consistent with the Commission's proposal — especially as contextual advertising is explicitly called out as a permitted use — but we believe the language should be made more clear. A failure to exempt the basic operational uses that plugin operators and other third parties make of users' IP addresses and other persistent identifiers would make it essentially impossible for these operators to comply with COPPA and could effectively prohibit first-party operators from using plugins and third-party services for rudimentary and unobjectionable purposes such as single-site analytics and contextual advertising.

IV. The Commission's Expansion of the Definition of Sites "Directed to Children" Is Vague and Threatens Free Expression

Commenters also have serious concerns about the Commission's second proposal to amend the definition of "directed to children" to introduce into the definition a category of sites that are "likely to attract an audience that includes a disproportionately large percentage of children." While this proposal would not, on its face, directly rescind COPPA's existing "actual knowledge" standard, the proposed change would accomplish the same shift to a "constructive knowledge" standard that Commenters have long argued against.[12] This proposal significantly widens the range of sites and services that will incur COPPA obligations, likely including both teen-oriented and general-audience sites that happen to appeal to children as well as adults. In previous rounds of comments, Commenters and many others[13] have cautioned the Commission that expanding COPPA's reach beyond sites directed primarily to an audience of children would raise concerns both for the First Amendment rights of adults and older minors to access information, and for the overall impact of the law on data collection from children

[12] *See* Joint Comments of Center for Democracy & Technology, The Progress & Freedom Foundation, and Electronic Frontier Foundation, June 30, 2010, (hereinafter CDT-PFF-EFF Joint Comments) *available at* www.ftc.gov/os/comments/copparulerev2010/547597-00050.pdf; CDT December 2011 Comments.

[13] *See, e.g.,* Comments of Tech Freedom, Dec. 23, 2011, *available at* http://www.ftc.gov/os/comments/copparulereview2011/00375-82401.pdf; Comments of Adam Thierer, Dec. 23, 2011, *available at* http://www.ftc.gov/os/comments/copparulereview2011/00337-82267.pdf; Comments of Facebook, Dec. 23, 2011, *available at* http://www.ftc.gov/os/comments/copparulereview2011/00369-82394.pdf, Comments of Family Online Safety Institute, Dec. 22, 2011, *available at* http://www.ftc.gov/os/comments/copparulereview2011/00312-82214.pdf..

and adult users.[14] The Commission's proposed definition raises precisely these same concerns.

First, the expanded definition of sites "directed to children" is too vague to provide operators with certainty about their obligations under the law. The current definition of "directed to children" – and the Commission's years of decisions interpreting and applying it – help to establish a clear line between the relatively small number of sites intentionally aiming their content at an audience of children under 13, and the rest of the general-audience sites and services on the Internet. [15] This level of certainty about COPPA's narrow scope is essential to operators' ability to comply with the law. The Commission's proposed new definition, however, would draw in sites that are "likely to attract an audience that includes a disproportionately large percentage of children under 13 as compared to the percentage of such children in the general population". The definition does not give operators guidelines as to what qualifies as "a disproportionately large percentage of children," requiring operators to make guesses both as to what proportion of their site visitors are children under 13, and whether that proportion is "disproportionately large".

Operators of teen-oriented sites, in particular, would likely face significant concerns that their sites could attract a "disproportionate" number of children. Sites intended for a teenage audience, such as the online version of the magazine *Seventeen*, often have aspirational appeal to younger children.[16] Under the proposed definition, *Seventeen*.com could be considered directed to children even though the magazine does not actively target children and does not know which of its users are children. Similarly, sites about sports, music, television, movies, or anything else with a general appeal to young people, would have to try to take close account of the relative proportions of their users. Facing this uncertainty, teen-oriented sites may respond by seeking to obtain parental consent for all of their users in order to avoid liability under COPPA. However, such a regime was struck down by the Supreme Court in *Brown v. Entertainment Merchants Association*, which prohibits restricting older minors' access to constitutionally protected speech.[17] The Commission's proposed carve-out for sites that conduct age-screening for all users also raises First amendment concerns, see *infra* part IV.

And, because COPPA obligations apply to "sites or portions thereof" that are directed to children, the proposed vague standard could pull any general-audience site that may have a page or piece of content particularly appealing to children into COPPA's scope. In particular, user-generated content sites, which appeal to a general audience but may have pages, videos, or other content that happens to be overwhelmingly popular with young children, will face new and unanticipated questions about their obligations under COPPA. It has never been the role of COPPA to require such general-interest sites to

---

[14] *See* CDT December 2011 Comments, *supra* note 12.

[15] *See* CDT-PFF-EFF Joint Comments, *supra* note 12 at 6 (discussing current definition of "directed to children").

[16] *See, e.g.*, Larry Magid, *Survey: Many Parents Help Kids Lie to Get on Facebook*, CNet (Nov. 1, 2011, 4:00 AM), http://news.cnet.com/8301-19518_3-20127633-238/survey-many-parents-help-kids-lie-to-get-on-facebook/ (discussing how children may want to be part of public debates and thus may create accounts with false age information, in some cases with their parents' consent).

[17] 131 S. Ct. 2729, 2736 (2011).

inventory all of the user-generated content they receive and assess it for its appeal to children, nor should it be.

Vague regulations that leave actors uncertain of their obligations under the law are vulnerable to constitutional challenges, particularly when the regulation may have a chilling effect on access to protected speech.[18] Vague regulations are likely to chill speech precisely because ordinary citizens cannot determine what conduct is permissible without sufficiently clear language.[19] In *Grayned v. Rockford*, for example, the Supreme Court noted that "where a vague statute '[abuts] upon sensitive areas of basic First Amendment freedoms,' it 'operates to inhibit the exercise of [those] freedoms.'"[20] As a result of unclear boundaries, citizens will inevitably "'steer far wider of the unlawful zone' [than] if the boundaries of the forbidden areas were clearly marked."[21] Operators facing uncertainty over when their sites or services might be deemed directed to children, and fearing the high costs associated with being found non-compliant,[22] will be discouraged from offering lawful, constitutionally protected content that might potentially appeal to children as well as the intended older audience.

Moreover, even if the Commission clarified exactly what percentage of children would make a site's audience "disproportionate" under the proposed definition, operators would still have no reliable way of knowing how their sites and services measure up. As many have noted,[23] users' age information is not automatically transmitted when they visit a site. Operators using basic analytics packages that limit the amount of data collected from users to a few pieces of information (e.g., an individual IP address) will know only general information about users' behavior on their site.[24] Such services do not purport to reveal age-based demographics for minors,[25] and it would be exceedingly difficult to

---

[18] *See, e.g.*, Kolender v. Lawson, 461 U.S. 352, 357 (1983).

[19] The "void for vagueness" doctrine specifies that there must be sufficient clarity and definition for ordinary people to understand what conduct is prohibited, and must prevent arbitrary enforcement. Connally v. General Construction Co., 269 U.S. 385, 391 (1926).

[20] 408 U.S. 104, 109 (1972).

[21] *Id.* at 109 & n. 5.

[22] Since COPPA was enacted, the Commission has undertaken several enforcement actions against operators who violated COPPA provisions. Damage awards have ranged from $10,000 to $3,000,000 in civil fines. *See* Federal Trade Commission, Legal Resources, http://business.ftc.gov/legal-resources/30/35. High fines from COPPA enforcement actions create obvious deterrence for other operators.

[23] *See, e.g.*, Comments of Yahoo, Dec. 23, 2011, http://www.ftc.gov/os/comments/copparulereview2011/00345-82371.pdf; Comments of eBay, Inc., Dec. 22, 2011, http://www.ftc.gov/os/comments/copparulereview2011/00328-82251.pdf.

[24] *See, e.g.*, User Report, *Google Analytics Integration of Demographic Data*, http://www.userreport.com/features/demographics-in-google-analytics/google-analytics-integration-2/. Some analytics providers use behavioral advertising in order to determine demographic information.

[25] Some analytics providers claim to be able to determine an "age range" for users, although such ranges do not extend to minors. *See, e.g.*, Google, *Reach People of Specific Age and Gender*, Sept. 6, 2012, https://support.google.com/adwords/bin/answer.py?hl=en&answer=2580383.

provide such information without more detailed data collection.[26] Estimated website demographic data, as the Commission itself has noted,[27] is notoriously unreliable, and operators cannot determine the age of their users without collecting specific data from those users. Site analytics packages that do claim to provide age categories as part of their demographics ask for information in user profiles, which may be unreliable.[28] In any case, more detailed analytics services that attempt to provide operators with detailed age demographics rely upon increased data collection and cross-site tracking of users – precisely the opposite of what the Commission hopes to accomplish.[29]

V. The Commission's Endorsement of Age Screening on General-Interest Sites and Services Exacerbates the Problem of Increased Data Collection and Puts COPPA on a Path that Is Both Inadvisable and Unconstitutional.

In the revised definition of "website or online service directed to children", the Commission creates a carve-out for sites that attract a disproportionately large percentage of children if such sites do not collect personal information prior to collecting age information. Rather than saving this vague standard, however, this carve-out only exacerbates the problems with the Commission's new approach.

The Commission does not provide specifics on how operators could avail themselves of this carve-out.[30] Instead, the Commission refers to "age screening", but does not go into further detail. Operators would not have a concrete sense of how much age or identity information they would need to collect from users, or how certain they would need to be in the accuracy of such information, in order to qualify for this carve-out. Currently, age screening generally takes the form of asking for date of birth or age, but this approach has noted weaknesses[31] and it is not clear whether this proposal would accomplish any real increase in protecting the privacy of children's personal information. More intrusive

---

[26] *See, e.g.*, Yahoo Web Analytics Blog, *Case Study: Demographic Insights with YWA*, Oct. 27, 2011, http://www.yanalyticsblog.com/blog/2011/10/case-study-demographic-insights-with-ywa/;.Google, *supra* note 25.

[27] See Supplemental Proposed Rule, *supra* note 3 at 59814.

[28] *See* INTERNET SAFETY TECHNICAL TASK FORCE, ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES: FINAL REPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE (hereinafter ISTTF Report), Appendix D at 28-31, Dec. 31, 2008, *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

[29] *Id.*; *see also* danah boyd, Eszter Hargittai, Jason Schultz, and John Palfrey, *Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the Children's Online Privacy Protection Act*, 16 FIRST MONDAY (2011), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075.

[30] Ironically, because the definition of sites that will attract a "disproportionately large percentage of children" is so vague, the effect of this new definition and carve-out may in fact be to create a loophole for operators of sites that currently fall under the definition of "directed to children". These operators may attempt to circumvent any COPPA obligations they should accrue by implementing some form of age screening and then arguing that their sites only attract a "disproportionate" number of children (rather than having an audience that is "primarily" children). While this result is clearly not the Commission's goal, it remains another drawback of the proposed language.

[31] *See, e.g.,* Supplemental Proposed Rule, *supra* note 3; danah boyd, Eszter Hargittai, Jason Schultz, and John Palfrey, *Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the Children's Online Privacy Protection Act*, 16 FIRST MONDAY (2011), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075.

age verification, or identity verification, carries with it a host of privacy and security concerns.[32]

Moreover, the decade-long litigation over the Child Online Protection Act (COPA) has demonstrated that a federal requirement to provide age or identity information prior to accessing constitutionally protected material online is a violation of the First Amendment. Under COPA, website operators were required to restrict minors' ability to access material deemed "harmful to minors." Operators would have been required to obtain age verification for all users who attempted to access such content.[33] In striking down COPA, the Third Circuit found that COPA was "substantially overbroad in that it place[d] significant burdens on Web publishers' communication of speech that is constitutionally protected as to adults and adults' ability to access such speech."[34]

The Commission's proposal is not, of course, a direct mandate for age verification à la COPA, but the inherent uncertainty in the "disproportionate" definition (as discussed above) will push operators who fear that their sites may be disproportionately appealing to children to seek the liability carve-out. Faced with a choice between potentially very high fines for non-compliance with COPPA's obligations[35] and implementing age screening, a great many operators will feel compelled to screen. But implementing age-screening technology places financial and resource burdens on operators, essentially leaving operators with a "choice" among three significant burdens: obtaining parental consent for all users, implementing age screening, or risking heavy fines. Each of these is a barrier to the ability of operators of general-audience sites, who are overwhelmingly dealing with content that is constitutionally protected not just for adults but for people of every age,[36] to express themselves. There is no question that the Commission's proposed revision will, in the words of the Third Circuit, "place significant burdens on Web publishers' communication of speech that is constitutionally protected."

Further, the age-screening process that operators will likely be compelled to implement will burden adults' and older minors' rights to access constitutionally protected content anonymously.[37] In the COPA cases, the Third Circuit determined that "requiring a user . . . to enter personal information prior to accessing certain material constitutes a much

---

[32] *See, e.g.*, ISTTF Report, Appendix D at 10.

[33] 47 U.S.C. § 231 (c)(1)(B) (2006). *See also* CDT-PFF-EFF Joint Comments, *supra* note 12, at 8.

[34] ACLU v. Ashcroft, 322 F.3d 240, 266 (3d Cir. 2003).

[35] Recent judgments (since 2010) in COPPA cases include $250,000 against Rock You, $100,000 against Skidekids, $50,000 against Broken Thumbs, and $3,000,000 against Playdom. *See* U.S. v. Rock You, No. 12-CV-1487 (N.D. Cal., Mar. 27. 2012) (consent decree and order), *available at* http://ftc.gov/os/caselist/1023120/120327rockyouorder.pdf; U.S. v. Godwin, No. 1:11-cv-03846-JOF (N.D. Ga., Feb. 1, 2012) (consent decree and order), *available at* http://www.ftc.gov/os/caselist/1123033/111108skidekidsorder.pdf; U.S. v. W3 Innovations, No. CV-11-03958 (N.D. Cal., Sep. 8. 2011) (consent decree and order), *available at* http://ftc.gov/os/caselist/1023251/110908w3order.pdf; U.S. v. Playdom, No. 11-0724-AG(ANx) (C.D. Cal., May 24, 2011) (consent decree and order), *available at* http://ftc.gov/os/caselist/1023036/110512playdomconsentorder.pdf.

[36] In *Brown v. EMA*, the Supreme Court held that the government cannot restrict minors' ability to access constitutionally protected speech. *Brown,* 131 S. Ct. 2729 (2011).

[37] ACLU v Ashcroft, 322 F.3d 240, 266 (3d Cir. 2003).

more severe burden on speech than technical difficulties"[38] and ultimately held age verification mandates would impermissibly require adults to relinquish their anonymity to access protected speech.[39] Again, as many operators would be unable to determine the percentage of children in their audience, and thus would have no certainty that they either were or were not within the "disproportionate" prong of the directed to children definition, many sites would avail themselves of the age-screening carve-out – the end result of the Commission's proposal being the widespread demand for personal information from all users prior to accessing constitutionally protected speech.

* * *

We appreciate the opportunity to comment on the Commission's supplemental proposed revisions to the COPPA Rule, and we look forward to working further with the Commission as it continues its review.

Respectfully submitted,

/s/

Justin Brookman
Emma J. Llansó
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, DC 20006
(202) 637-9800
jbrookman@cdt.org
ellanso@cdt.org

September 24, 2012

[38] *Id.* at 259.

[39] *See* ACLU v. Mukasey, 534 F.3d 181, 197 (3d Cir. 2008); Joint Comments, *supra* note 33, at 8.