Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
Room H-113 (Annex E)
600 Pennsylvania Avenue NW
Washington, DC 20580

RE: COPPA Rule Review, 16 CFR Part 312, Project No. P104503

Dear Secretary Clark:

Facebook appreciates the Commission's ongoing engagement in the important area of children's privacy. By soliciting comments on its most recent proposed changes to the Rule implementing the Children's Online Privacy Protection Act ("COPPA"), the Commission has demonstrated its commitment to ensuring a free and open debate on issues that will shape children's online experiences for years to come.

We applaud the Commission's thoughtful review of the comments it has received to date. The voluminous record that has developed during the course of this rulemaking shows that changes to the COPPA Rule that seem simple in theory could have unintended and profound effects in practice. Today's websites and online service providers give children and teens access to an unprecedented variety of resources to foster and support teaching and learning.[1] These resources "are an important element of an infrastructure for learning and range from podcasts to digital libraries to textbooks and games."[2]

A highly-lauded example of such resources is Khan Academy, "a not-for-profit organization providing digital learning resources, including an extensive video library, practice exercises, and assessments."[3] Khan Academy "has had 179 million video views so far" and "is supported by donors such as Google and the Bill and Melinda Gates Foundation."[4] The site enriches and supplements students' educational experiences by providing them with multimedia educational content. This resource gives parents and teachers the ability to review students' progress and relevant statistics in real time, and supplies students with "badges" that provide motivation and positive reinforcement by

---

[1] *See, e.g.*, U.S. Dep't of Ed., Use of Technology in Teaching and Learning, http://www.ed.gov/oii-news/use-technology-teaching-and-learning (last visited Sept. 21, 2012).

[2] *Id.*

[3] *Id.*

[4] Bruno B.F. Faviero, Major Players in Online Education Market: Comparing Khan Academy, Coursera, Udacity, & edX Missions, Offerings, Tech Online Edition (Sept. 4, 2012), http://tech.mit.edu/V132/N34/education.html.

allowing them to share their progress on third-party social media sites like Facebook.[5] Khan Academy, of course, is just one of many websites and online services developing content that is vital to the technological education and advancement of minors.

As the Commission evaluates the further changes proposed in the Supplemental Notice of Proposed Rulemaking ("SNPRM"), Facebook encourages the Commission to develop policies that take into account the significant impediments that a revised COPPA Rule could create for innovation and the ecosystem that shapes students' online experiences. This social functionality, widely used by educational sites and apps,[6] is dependent on plugins and could be threatened by a COPPA Rule that renders plugin providers responsible for the actions and motives of third parties and vice versa. Part of the value of many educational sites and services is that they are offered for little or no cost, which means that they often will not have the resources to meet burdensome compliance obligations.[7] Requiring these sites or services and plugin providers to monitor each others' information practices could result in the eradication of integrated plugins and the powerful features they facilitate. Furthermore, barring sites and online services from using platforms or common mechanisms to comply with their COPPA obligations could chill innovation due to the cost of compliance.

Facebook believes strongly in the importance of empowering parents to protect their children online, and we have been leaders in efforts to promote the safety of the minors, aged 13 to 17, who use our service. However, we have serious concerns that the confluence of changes proposed in the SNPRM—the expansion of the definition of "operator," the potential for plugin providers to be subject to COPPA based on actions of website publishers of which they are unaware, and the lack of clarity around whether a plugin provider will violate COPPA by using data collected in order to operate the service of which the plugin is a part—all dramatically increase the risks faced by entities that wish to distribute plugins and other tools that enhance the utility and value of the Internet. In the aggregate, these changes exceed the authority that Congress granted to the Commission in COPPA. Just as Congress worried that unchecked liability would stifle the growth of the Internet when it adopted Section 230 of the Communications Decency Act and the Digital Millennium Copyright Act's safe harbor provisions, the absence of clear standards around the circumstances under which liability attaches under COPPA is likely to create serious disincentives against growth in Internet technologies.

When COPPA was enacted in 1998, both Congress and the Commission expressly recognized that interactive online experiences could promote children's growth and development. Since that time, the benefits of interactive media to children have become even clearer: providing personalized learning experiences, teaching skills vital to success in the modern workplace, and creating new communication tools to foster creativity and deepen social connections. In light of the benefits to children from having

---

[5] Khan Academy, About, http://www.khanacademy.org/about (last visited Sept. 21, 2012).

[6] The Project Noah site allows students to become "citizen scientists" and document and share the wildlife they encounter. *See* Project Noah, http://www.projectnoah.org/ (last visited Sept. 21, 2012). Popplet won an award from the American Association of School Librarians for its app that allows students to organize and share ideas. *See* Popplet, Popplet Named in Top 25 List of Best Websites for Teaching and Learning, Poppletrocks! (July 5, 2012), http://blog.popplet.com/popplet-named-in-top-25-list-of-best-websites-for-teaching-and-learning/. Codecademy allows students to learn to program in numerous technologies. Codecademy, Tracks, http://www.codecademy.com/learn (last visited Sept. 21, 2012). All three have integrated plugins.

[7] While some of these sites are operated by non-profit enterprises that are not subject to the COPPA Rule, others are for-profit sites that are supported through other business models.

access to interactive online services and given the scope and intent of COPPA, our comments recommend that the Commission consider three key issues to ensure the final Rule advances COPPA's goals:

1. **Liability.** The Commission should decline to impose liability on plugin providers based on the independent actions of website publishers, and vice versa. This is because—
   - Plugin providers operate independently of website publishers, not on their behalf, to provide important benefits to users;
   - COPPA precludes liability for general-audience plugin providers absent actual knowledge;
   - An operator cannot be liable when it age screens and knows that it is collecting information from an individual age 13 or older; and
   - The Commission's proposal raises First Amendment concerns.

2. **Support for Internal Operations.** The Commission should recognize that, even if plugins on child-directed properties were subject to the COPPA Rule, the definition of "support for internal operations" must cover data collected by plugins and explicitly include activities that do not impact children's privacy.

3. **Common Mechanisms.** The Commission should modify the COPPA Rule to be consistent with the statute and to clarify that multiple operators participating in a single platform may use a common mechanism to satisfy certain of their COPPA obligations, with each retaining full responsibility to parents and the Commission for their own independent actions.

Facebook strongly supports the Commission's goal of encouraging collaboration between various participants in the online ecosystem to empower parents to manage their children's Internet use. In the context of these three key issues, our comments focus on that goal and make recommendations that allow the Commission to support and foster an innovative and robust ecosystem for families on the Internet.

I. The Commission Lacks Statutory Authority to Impose Liability on Plugin Providers and Website Publishers for Each Others' Independent Decisions.

Plugins are small pieces of computer code that display an instance of one website within a page displayed by another website. They provide a lightweight and convenient way for website publishers—particularly those with limited resources—to add dynamic features, such as interactivity, videos and other multimedia content, and advanced functionality, to their websites in order to enhance the usability and value of the Internet experience.

In enacting COPPA, Congress sought to achieve two distinct but complementary goals: "to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment" *and* to "preserve[] the interactivity of children's experience on the Internet and . . . children's access to information in this rich and valuable medium."[8] Facebook is concerned that certain changes proposed in the SNPRM would improperly pursue the first of these goals at the expense

[8] 144 Cong. Rec. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan). Senator Bryan was one of COPPA's primary sponsors.

of the second. As the Commission has observed,[9] it is possible to empower parents to protect the privacy of their children while creating incentives for companies to provide innovative and valuable services for children such as those enabled by plugins.

The Commission can and should pursue both of these goals at the same time by making three changes to the proposal in the SNPRM regarding joint liability of plugin providers and the publishers of websites on which the plugins appear: *First*, the Commission should revise the "on behalf of" language in the definition of "operator" to be consistent with COPPA's statutory text. *Second*, the Commission should decline to hold plugin providers liable under COPPA except when their independent practices otherwise trigger COPPA. *Third*, the Commission should make clear that it will not undertake COPPA enforcement against entities that have age screens and know that they are collecting information from individuals age 13 or older.

A. Plugins Operate Independently of Website Publishers, Not on Their Behalf, to Provide Important Benefits to Users.

Under the proposed Rule announced in the SNPRM, website publishers and app developers that integrate other services that collect personal information from visitors on their child-directed sites and services will be deemed "co-operators" with the integrated services for purposes of COPPA. In the Commission's view, even if the child-directed site or service does not own, control, or have access to the personal information, the personal information is collected "on its behalf" because the child-directed site or service "benefits from its use of integrated services that collect personal information" to the extent that the integrated services provide the site with "content, functionality, and/or advertising revenue." The Commission therefore proposes to add a proviso to the "operator" definition, specifying that "[p]ersonal information is collected or maintained on behalf of an operator where it is collected in the interest of, as a representative of, or for the benefit of, the operator."[10]

The Commission's proposed approach fundamentally misunderstands the relationship between plugin providers and website publishers. Facebook, like other plugin providers, makes plugins available for any website publisher or app developer to use. Our plugins are available in a "stock" form that enables publishers of other websites to add social functionality to their sites unilaterally, without customization by Facebook. We do not select the websites that choose to use our plugins, which plugins they use, or whether they install the plugins on all or only some of their pages (*e.g.*, only those pages directed toward parents). Those decisions are entirely controlled by the website publisher, and we do not review or vet websites before their publishers install our plugins. If publishers choose to install our plugins, Facebook generally delivers personalized content directly to the user's browser, which then displays the Facebook content alongside the content from the website publisher. Additionally, although plugin providers supply functionality that complements the websites on which their plugins appear, and even though the two appear on the same display, they are distinct services.

---

[9] *See, e.g.*, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804, 59,808 (Sept. 27, 2011) ("The Commission has undertaken this Rule review with an eye towards encouraging the continuing growth of engaging, diverse, and appropriate online content for children that includes strong privacy protections by design. Children increasingly seek interactive online environments where they can express themselves, and operators should be encouraged to develop innovative technologies to attract children to age-appropriate online communities while preventing them from divulging their personal information.").

[10] Children's Online Privacy Protection Rule, 77 Fed. Reg. 46,643, 46,644 (proposed Aug. 6, 2012).

Generally, plugin providers do not collect data at the direction of the website publisher, and they do not as a matter of course share collected data with that entity. When users interact with our social plugins, we collect data to be used in our own service—for example, to enable users to post content to their Facebook Timelines. And, unless a user specifically chooses to share with a website (for example, using a Facebook Login plugin to create an account with the website), we generally do not pass plugin data to the website publisher. In this manner, social plugin technology enables the user to communicate with two distinct entities on a single page.

Given these facts, it is implausible to suggest that a plugin provider is acting "in the interest of, as a representative or, or for the benefit of" the website publisher. Under the statute, the term "operator" is defined to mean "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."[11] Although Congress did not define the term "on behalf of," standard principles of statutory interpretation require that the term be given a much narrower construction than the interpretation proposed in the SNPRM.

1. Counter to Statutory Language. Because Congress chose not to define the phrase "on behalf of," the phrase should be given its ordinary meaning.[12] The common meaning of "on behalf of" limits the term to entities that are acting as agents or representatives. For example, *Webster's New College Dictionary* defines "on behalf of" to mean "[o]n the part of: speaking for."[13] Similarly, the *American Heritage Dictionary* defines "on behalf of" to mean "[a]s the agent of," and *Merriam-Webster* defines the term to mean "as a representative of."[14] Plugin providers are not acting "on behalf of" website publishers or app developers when the publisher or developer uses their plugins, because plugin providers are not agents or representatives of the publisher or developer. Rather, as noted above, plugin providers make their plugins available for "off-the-shelf" use by any website publisher or app developer who wishes to add plugin functionality to a website or app. In addition, the personal information that plugin providers collect is primarily for their own benefit, not for the benefit of the hosting website. It therefore would be inappropriate to deem publishers or developers to be "operators" based solely on the fact that plugin providers might collect personal information via plugins on the publisher's or developer's website or app.

2. Counter to Legislative History. COPPA's legislative history provides further evidence that the "on behalf of" language was intended to cover traditional principal-agent relationships. In explaining the "operator" definition, Senator Bryan, one of COPPA's chief sponsors, stated, "This term is defined as the person or entity who both operates an Internet website or online service and collects information on that site either directly *or through a subcontractor*. This

[11] 15 U.S.C. § 6501(2).

[12] *See, e.g.*, *FDIC v. Meyer*, 510 U.S. 471, 476 (1993) ("The term 'cognizable' is not defined in the Act. In the absence of such a definition, we construe a statutory term in accordance with its ordinary or natural meaning.").

[13] *Webster's New College Dictionary* 102 (2008).

[14] *American Heritage Dictionary* 79 (4th ed. 2001); *Merriam-Webster Dictionary* (11th ed. 2004).

definition is intended to hold responsible the entity that collects the information, as well as the entity on whose behalf the information is collected."[15]

3. Counter to Common Legal Usage and Interpretation. The proposed proviso is a significant departure from other privacy laws and regulations that use the term "on behalf of" more narrowly. For example, the Gramm-Leach-Bliley Act ("GLBA") recognizes that a nonaffiliated third party acts "on behalf of" a financial institution when the third party performs services for the financial institution, such as marketing the financial institution's own products and services.[16] If the standard applied in the SNPRM were to be applied in the GLBA context, then financial institutions would be permitted to freely share nonpublic personal information with a third party without providing the statutory consumer disclosure form, so long as the third party provided some benefit to the financial institution—for example, by paying the financial institution for the personal information. This result clearly would be inconsistent with the purpose of GLBA. Similarly, the SNPRM would be inconsistent with the regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA"). In the HIPAA context, a business associate acts "on behalf of" a covered entity when it "performs or assists [the covered entity] in the performance of" regulated functions or activities.[17] As these other privacy laws and regulations make clear, entities acting primarily for their own benefit are not considered to be acting "on behalf of" another party.

Furthermore, statutes should not be interpreted in a way that would lead to an absurd result[18]—which is precisely what the proposed proviso would do. The language in the SNPRM could encompass a variety of third parties that Congress never intended to subject to COPPA. For example, the SNPRM could be read broadly to capture Internet Service Providers ("ISPs"). Websites "benefit" from ISPs, because they provide websites with "functionality"—a user who does not have an ISP will not be able to visit the site. In addition, ISPs collect IP addresses and other information to, for example, deliver content and filter out potentially malicious websites. Consequently, the Commission's proposal would lead to a fundamentally illogical conclusion: any time a child user visits a website, the website publisher would be deemed a covered operator who is required to comply with COPPA, simply because the publisher benefits from the services provided by the child user's ISP.

To ensure consistency with COPPA, the Commission should narrow the proviso to clarify that an entity acts "on behalf of" another entity only if it is acting as the agent of that other entity. Instead of adding the overly broad language proposed in the SNPRM, the Commission should clarify that personal

---

[15] 144 Cong. Rec. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan) (emphasis added).

[16] 15 U.S.C. § 6802(b)(2) ("This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions *on behalf of* the financial institution, including marketing of the financial institution's own products or services, or financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with the requirements imposed by the regulations prescribed under section 6804 of this title, if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information." (emphasis added)).

[17] 45 C.F.R. § 160.103.

[18] *See, e.g.*, *United States v. Granderson*, 511 U.S. 39, 47 n.5 (1994) (dismissing an interpretation on the ground that it "leads to an absurd result").

information is collected or maintained on behalf of an operator only if it is collected by a representative or agent of the operator. This revision would be consistent with the plain meaning of the term, COPPA's legislative history, and other privacy laws and statutes—and it would also provide clearer guidance to entities seeking to understand whether they are subject to COPPA or not. Specifically, the Commission should modify the proposed proviso in the definition of "operator" in Section 312.2 of the COPPA Rule as follows:

> Personal Information is *collected or maintained on behalf of* an operator where it is collected ~~in the interest of, as~~ by a representative or agent of~~, or for the benefit of,~~ the operator.

As a matter of best practices, child-directed sites that already have a process in place whereby they provide notice and obtain parental consent might consider also disclosing and obtaining consent for plugins and similar technologies because doing so would promote greater understanding of how the online ecosystem operates. But the Commission does not have the legal authority to make this a regulatory *requirement*.

B. COPPA Precludes Liability for General-Audience Plugin Providers Absent Actual Knowledge.

Based on the faulty assumption that plugin providers act "on behalf of" website publishers, the Commission proposes to expand dramatically the scope of the COPPA Rule by concluding that the providers of plugins are "co-operators" with website publishers, even where the plugin provider lacks actual knowledge that it is collecting personal information from a child under the age of 13. Under the Commission's proposal, such a provider might be liable if it has a mere "reason to know" that a website on which its plugin is placed is child-directed.

Even if a plugin provider did act "on behalf of" website publishers—which, as noted above, it in almost all cases does not—the plain language of the COPPA statute unambiguously forbids this interpretation. An operator of a general-audience website or service is subject to COPPA only if it has "actual knowledge that it is collecting personal information from a child."[19] Absent actual knowledge, COPPA can only be applied to operators whose own websites or online services are directed to children.

Significantly, plugin providers do not operate the websites on which they appear as third parties.[20] Instead, they independently operate their own websites or online services. Facebook's online service is directed to a general audience. We do not knowingly collect personal information from children, and we use practices recommended by the Commission in an effort to prevent children from joining our service. In addition, when we learn that a particular Facebook user is a child, we take steps to disable the account and delete information submitted by that child. The fact that some child-directed

[19] 15 U.S.C. § 6502(a)(1). The legislative history confirms that Congress intended COPPA to create obligations for general-audience operators only to the extent that they have actual knowledge that they are collecting personal information from a child under the age of 13. *See* 144 Cong. Rec. S11,658 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan) ("The regulations shall apply to any operator of a website or online service that collects personal information from children and is directed to children, or to any operator *where that operator has actual knowledge that it is collecting personal information from a child*." (emphasis added)).

[20] 15 U.S.C. § 6502(a)(1).

websites or services choose to use Facebook's plugins does not convert our plugins into a "portion of a commercial website or online service that is targeted to children," as the SNPRM appears to suggest. Regardless of the publisher's or developer's intended audience, the intended audience for Facebook's plugins—which is the only relevant audience for determining whether that "portion" of Facebook's service is directed to children and therefore subject to COPPA—is and always remains a general audience. The fact that a publisher or app developer avails itself of Facebook's plugins on sites and services that are child-directed does not—and cannot under the statute—affect the analysis of whether *Facebook* is a child-directed site or service. Consequently, Facebook remains directed to a general audience, even when child-directed websites choose to deploy our plugins.

The Commission does not define what it means when it says that a plugin provider may have a "reason to know" that its plugins appear on a website or online service that is child-directed, but ultimately any "reason to know" standard would be fatally unworkable in this context, even if it was statutorily permissible, for several reasons.

1. Unworkable Obligation to Prescreen Sites. As the SNPRM acknowledges, it would be impracticable to require a plugin provider to investigate each domain on which its plugins appear or to adjudicate in advance whether the particular URL is for a child-directed page. Given that Facebook offers its plugins for "off-the-shelf" use by many thousands of website publishers, we agree with the Commission that Facebook and other plugin providers would face significant "logistical difficulties … in controlling or monitoring which sites incorporate their online services," and it would be "unworkable" to impose liability on plugin providers for the activities of the publishers on whose sites their plugins appear.[21]

2. Unworkable Obligation to Investigate Complaints. It also would not be feasible for plugin providers to undertake an investigation each time they receive a complaint or allegation that a website or service using their plugins is child-directed. The Commission currently applies a qualitative, fact-specific, totality-of-the-circumstances test that considers ten non-exclusive factors to determine whether a website is child-directed, and the 2011 NRPM proposes to add an eleventh factor to the list. Plugin providers cannot be expected to apply this multi-factor test every time they receive a complaint or allegation that a child-directed website is employing their plugins. Such a requirement would impose an unreasonable burden on plugin providers, especially because some of these factors rely on information that is unavailable to the plugin provider. Additionally, the Commission's proposal would create an incentive for plugin providers to collect and store *more* data about the people who use their services in order to counter any allegations of child-directedness that they receive—a result that undermines COPPA's goal of discouraging the collection of information about children.

The SNPRM also leaves open many questions about the circumstances in which the plugin provider will be deemed to have sufficient knowledge to create liability. For example, it is unclear what happens if the plugin provider decides in good faith that the website hosting the plugins is not child-directed but a complainant or the Commission reaches the opposite conclusion, or if the hosting site shifts its focus or content after the plugin provider's investigation has been concluded. There is no reasonable basis to hold the plugin provider liable

[21] 77 Fed. Reg. at 46,645.

in those circumstances, and to do so would only discourage providers from making plugins available for use by other companies—a result that plainly disserves the public interest.

3. Unworkable Definition of "Personal Information." Even assuming that the plugin provider has sufficient information to determine whether a website or service is child-directed (which will be the exception rather than the rule), it is unclear how the plugin provider must respond. The revised COPPA Rule would expand the definition of "personal information" to include the collection of "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier" from a child.[22] COPPA authorizes the Commission to continue to evaluate the definition of "personal information" to include identifiers that the Commission determines "permits the physical or online contacting of a specific individual."[23] Congress understood that, as technology develops, the definition of personal information might need to be updated. But such updates must be consistent with the intent of Congress to involve parents only when websites and online services that either focus on children or know they are collecting information from children directly interact with those children. Certain persistent identifiers received by plugin providers do not meet COPPA's statutory definition of "personal information" because such identifiers do not allow for the identification or contacting of a specific individual unless they are combined with other elements of personal information.[24]

Further, the Commission's attempt to broaden the definition of "personal information" on the basis that persistent identifiers permit identification and direct contact of children under 13 would undermine COPPA's goals by requiring operators to collect *more*, not less, personal

---

[22] 77 Fed. Reg. at 46,647.

[23] 15 U.S.C. § 6501(8)(F).

[24] *See* Interactive Advertising Bureau, In re COPPA Rule Review 6 (Dec. 23, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00359-82385.pdf ("Without additional data, there is no realistic way to link a persistent IP address, cookie data, or device identifier back to a specific individual or to use such identifiers to contact an individual. A company that uses persistent identifiers for browsers has no more 'contact' with a specific, named visitor than a company that places an advertisement in a children's magazine has 'contact' with a specific child subscriber."); Microsoft Corp., In re COPPA Rule Review 9 (Dec. 23, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00326-82245.pdf ("An operator that collects a persistent cookie ID from the user's device or computer cannot subsequently use that persistent identifier to 'contact' the individual – at least not in the ordinary sense of the word. At most, the persistent identifier enables the entity that sets the cookie to recognize the device if and when the device returns to the website or visits another website within the entity's network."); Motion Picture Association of America, In re COPPA Rule Review 12 (Dec. 23, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00362-82388.pdf ("Acquisition of an Internet Protocol ('IP') address, a customer number held in a cookie, a processor, device serial number, or a unique device identifier does not give the possessor of that information the means to contact users of the devices associated with those identifiers."); Yahoo! Inc., In re COPPA Rule Review 5 (Dec. 23, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00345-82371.pdf ("[T]he persistent identifiers used in this model (e.g., persistent identifiers in cookies, mobile device identifiers, and IP addresses) cannot be used to directly contact or even identify specific *individuals* unless they are combined with associated *personally identifiable information*, such as an individual's name, address, email address, or mobile phone number. Historically, this use of unique identifiers has been privacy-protective, as it allowed companies to assess users' activity without having to create databases containing personally identifiable information that could cause potential harm to users if stolen or lost.").

information in order to request parental consent. It would also prove unworkable because it is not consistent with the way in which websites and online services operate today.[25] Due to the existing architecture of the Internet, plugin providers receive information—including an IP address—from a user's browser the moment it connects to their servers, as the browser loads the page the user is viewing. Consequently, plugin providers would receive "personal information," and arguably fall within the statute's scope, involuntarily and without any opportunity to provide notice and obtain consent prior to the collection of this information. Consequently, it is both inadvisable and impracticable to interpret COPPA as requiring website publishers and plugin providers to obtain verifiable parental consent before a child may access a home page or other webpage where a plugin is used, because such access would immediately and automatically result in the collection of the child's IP address.[26]

Congress designed COPPA to avoid creating unchecked liability for operators that did not intend to violate the statute. Specifically, COPPA requires an intentional act by an operator before liability attaches: either the operator must have actual knowledge that it is collecting personal information from a child, or it must intentionally direct its service to children and collect personal information. This approach reflects Congress's understanding that the costs of imposing liability absent intentional misconduct are significant. The Commission's proposal to hold plugin providers liable for the targeting decisions of websites on which their plugins appear fundamentally upends that judgment by imposing liability even when a plugin provider may not know that COPPA is implicated.

For these reasons, Facebook respectfully requests that the Commission decline to adopt the proposed "reason to know" standard and instead, consistent with the statute, hold general-audience plugin providers liable under COPPA only when they have actual knowledge that they are collecting personal information from a child under 13.

C. An Operator Cannot Be Liable When It Age Screens and Knows That It Is Collecting Information from a Person Age 13 or Older.

In the SNPRM, the Commission states that "[t]he effect of the proposed changes would be that those sites and services at the far end of the 'child-directed' continuum, *i.e.,* those that knowingly target, or have content likely to draw, children under 13 as their primary audience, must still treat all users as children, and provide notice and obtain consent before collecting any personal information from any user."[27] Consequently, outside the proposed category of "child-friendly mixed audience" sites and services that may explicitly age screen, the revised COPPA Rule would require operators on child-directed sites (whether the publisher of the site or a social plugin provider integrated on the site) to obtain parental consent for all users of those sites, even if they have actual knowledge that a particular user is 13 years old or older.

---

[25] The Commission incorrectly concluded that "increasingly, consumer access to computers is shifting from the model of a single, family-shared, personal computer to the widespread distribution of person-specific, Internet-enabled, handheld devices to each member within a household, including children. . . . [O]perators now have a better ability to link a particular individual to a particular computing device." 76 Fed. Reg. at 59,811-12. Because more and more common household devices, such as televisions and video game consoles, are Internet-enabled, it remains difficult to link particular individuals to particular computing devices.

[26] See Section II, *infra*.

[27] 77 Fed. Reg. at 46,646.

This proposal exceeds the clear intent of Congress, which was to limit COPPA's obligations to situations in which "personal information [is] collected *from a child*."[28] This language excludes from the statute's enhanced obligations any circumstances in which an operator collects information from a teenager or adult. Accordingly, just as an operator can be held liable if it has actual knowledge that it is collecting information "*from a child*" on a general-audience website, an operator is necessarily outside the scope of COPPA when it collects information from an individual that it knows to be age 13 or older.

The statute similarly limits the Commission's COPPA rulemaking authority to situations involving the collection of personal information *from a child*. Specifically, the statute grants the Commission the following authority:

> Not later than 1 year after October 21, 1998, the Commission shall promulgate under section 553 of title 5 regulations that—
>
> (A) require the operator of any website or online service directed to children that collects personal information *from children* or the operator of a website or online service that has actual knowledge that it is collecting personal information *from a child*—
>
> . . .
>
> (ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information *from children*.[29]

This clear statutory language precludes the Commission from regulating the collection, use, or disclosure of personal information from a user who is 13 years of age or older, even if this collection or disclosure occurs on websites that are directed to children. This conclusion is supported by the legislative history. In the words of Senator Bryan: "The regulations shall apply to any operator of a website or online service that collects personal information from children *and* is directed to children, or to any operator where that operator has actual knowledge that it is collecting personal information from a child."[30] The Commission does not have the authority to adopt a regulation that conflicts with a statute that clearly expresses Congress's intent.[31] Indeed, courts reviewing agency actions are required to "hold unlawful and set aside agency action, findings, and conclusions found to be . . . in excess of

---

[28] 15 U.S.C. § 6501(4) (defining "disclosure" to require that the personal information that is released or made publicly available be "collected *from a child*" (emphasis added)); *id.* § 6501(9) (specifying that the mechanism must "ensure that a parent *of a child* receives notice" and that the notice is provided "before that information is collected *from that child*" (emphases added)); *id.* § 6502(a)(1) (making it "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*" (emphasis added)).

[29] *Id.* § 6502(b) (emphasis added).

[30] 144 Cong. Rec. S11,658 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan) (emphasis added).

[31] *Chevron v. Natural Resources Defense Council*, 467 U.S. 837, 842-43 (1984) ("First, always, is the question 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.").

statutory jurisdiction, authority, or limitations, or short of statutory right."[32] Facebook respectfully suggests that a court would do so here, if the Commission adopted a rule that imposed obligations on entities when they collect information from individuals they know to be age 13 or older.

Even if the statute was ambiguous (which it plainly is not), the proposed approach could not stand, as it is unreasonable and unworkable. A non-trivial number of users of child-directed websites will be teens and adults, including parents. It would be nonsensical to require an operator to obtain verifiable parental consent before collecting information from a parent. In addition, since the Commission first implemented the COPPA Rule in 1999, the Commission has taken the position that operators of general-audience sites have "actual knowledge" that a user is under 13 if "registration or other information reveals that the person ... is a child."[33] The Commission has affirmed, through frequently asked questions published on its website and its enforcement actions, that neutral age screens are a means for an operator of a general-audience site or service to obtain "actual knowledge" of a user's age.[34] In short, the Commission has long considered age information provided through a neutral age screen to be a reliable means of ascertaining a user's age. Facebook, like millions of other general-audience sites, has relied on this guidance from the Commission in designing our registration flow and neutral age-gate process. For registered Facebook users, Facebook has actual knowledge that the user is at least 13 years old because he or she has provided a birthdate during the registration flow indicating an age of 13 years of age or older.[35]

The SNPRM confirms that a neutral age-gate process is an appropriate and reliable means of determining a user's age, even on child-directed sites and services. Specifically, the SNPRM proposes that operators of child-friendly, mixed-audience sites that age-screen all users will be "deemed to have actual knowledge" that a given user is less than 13 years old only if the user identifies him- or herself as under 13 years of age.[36] While acknowledging that "many children may choose to lie about their age," the Commission concluded that "the proposed revisions strike the correct balance" and acknowledged that age gates are reliable because, in the "Commission's law enforcement experience . . . many children do truthfully provide their age in response to an age screening."[37]

---

[32] 5 U.S.C. § 706(2)(C); *see also Katharine Gibbs School (Inc.) v. FTC*, 612 F.2d 658, 665 (2d Cir. 1979) (striking down provisions of a Commission rule "[b]ecause the Commission is attempting to exercise a power 'inconsistent and at variance with the over-all purpose and design of the Act'").

[33] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,890 (Nov. 3, 1999).

[34] *See, e.g.*, FTC, Frequently Asked Questions About the Children's Online Privacy Protection Rule, FAQ # 38, http://www.ftc.gov/privacy/coppafaqs.shtm#teen (last visited Sept. 21, 2012) ("Although you may intend for your site to target only teenagers, your site still may attract a substantial number of children under 13. A teen-directed site can identify which visitors are under 13, for example, by asking age when visitors are invited to provide personal information.").

[35] In addition to obtaining actual knowledge about a user's age through this neutral age-gate process, Facebook takes a number of voluntary steps to help ensure that users are not under the age of 13. For more information about the technical and community-based tools that we use to identify child accounts, please see our December 2011 submission.

[36] 77 Fed. Reg. at 46,646.

[37] *Id.*

The Commission must "strike the correct balance" in a manner that is consistent.[38] It would be arbitrary and capricious for the Commission to conclude that an operator has "actual knowledge" when a question is answered on one site but lacks "actual knowledge" when the same question is answered on a different site. This is especially true when the Commission has itself acknowledged that any inaccuracy in the answer to an age-gating question does not detract from the conclusion that the answer creates "actual knowledge."

For example, it would be illogical to require a plugin provider who has collected reliable information about a user's age during a registration process on its general-audience website or service to disregard this age information simply because the user happens to navigate to a child-directed site where its plugin is integrated. If a teen registers on Facebook.com (which is directed to a general audience) and provides age information indicating that he or she is at least 13 years old (which, as explained above, the Commission has always found to be reliable), and then (while still logged in) navigates to a third party's child-directed website where a Facebook plugin is integrated, it would be unreasonable for that reliable age information to suddenly be deemed unreliable solely because the user visited a different website.

For these reasons, the suggestion in the SNPRM that operators of child-directed sites or services must "treat all users as children," even if the operator has actual knowledge that a particular user is 13 years old or older, would be "arbitrary and capricious" in violation of the Administrative Procedure Act.[39] Consequently, the Commission should clarify that any presumption that users of child-directed sites are children may be overcome by actual knowledge that a particular user is a teen or an adult.

D. The Commission's Proposal Raises First Amendment Concerns.

Because the Commission's proposal would restrict the ability of users who are 13 years old or older to "Like," comment on, or recommend the websites or services on which those plugins are integrated, it would infringe upon their constitutionally protected right to engage in protected speech.

As we and others have explained elsewhere, a user's decision to click on a social plugin is constitutionally protected speech that generates expressive content on the user's Profile (or Timeline) Page, as well as similar content in the News Feeds of the user's Friends.[40] The Supreme Court has

---

[38] *See Portland Cement Ass'n v. EPA*, 665 F.3d 177, 188 (D.C. Cir. 2011) ("'When an agency . . . is vested with discretion to impose restrictions on an entity's freedom to conduct its business, the agency must exercise that discretion in a well-reasoned, consistent, and evenhanded manner.'" (quoting *Greyhound Corp. v. ICC*, 668 F.2d 1354, 1359 (D.C. Cir. 1981))); *FERC v. Triton Oil & Gas Corp.*, 750 F.2d 113, 116 (D.C. Cir. 1984) ("Agencies must implement their rules and regulations in a consistent, evenhanded manner.").

[39] *See Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) ("[A]n agency rule would be arbitrary and capricious if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.").

[40] *See* Brief of Facebook as Amicus Curiae in Support of Plaintiff-Appellant Daniel Ray Carter, Jr., and in Support of Vacatur, *Bland v. Roberts*, No. 12-1671 (4th Cir. Aug. 6, 2012); Brief of Amici Curiae American Civil Liberties Union & ACLU of Virginia in Support of Plaintiffs-Appellants' Appeal Seeking Reversal at 5-10, *id*.

recognized on numerous occasions that teens are entitled to First Amendment protection.[41] Furthermore, the Court has held that statutes should be interpreted to avoid raising constitutional problems.[42] A government regulation that restricts teens' ability to engage in protected speech—as the proposed COPPA Rule would do—raises issues under the First Amendment.

To avoid this serious concern and the others raised above, the Commission should refrain from adding proposed new paragraph (d) in the definition of "website or online service directed to children." Instead, the Commission should clarify that, while it intends to "hold the child-directed property … equally responsible … for personal information collected by the plug-in," this is only true in cases where the plugin provider itself is subject to COPPA—*i.e.*, because the plugin provider directs its services to children or has actual knowledge that it is collecting personal information from a child. In these situations and only these situations, the plugin provider would be required to abide by COPPA's requirements. Specifically, the Commission should add a proviso to the definition of "website or online service directed to children" in Section 312.2 of the COPPA Rule, as follows:

> *Web site or online service directed to children* means a commercial Web site or online service, or portion thereof, that:
>
> . . .
>
> ~~(d) knows or has reason to know that it is collecting personal information through any Web site or online service covered under paragraphs (a)-(c).~~
>
> . . .
>
> A commercial Web site or online service, or a portion thereof, shall not be deemed directed to children solely because it provides technology to a commercial Web site or online service directed to children, unless the Web site or online service providing the technology is itself directed to children.

II. The Definition of "Support for Internal Operations" Should Be Clarified to Capture Data Collected by Plugins and to Explicitly Include Activities That Do Not Impact Children's Privacy.

The proposed COPPA Rule would amend the definition of "personal information" so that a "persistent identifier" (*e.g.*, an IP address or cookie ID) would not be deemed "personal information" if used solely for functions that provide "support for internal operations." "Support for internal operations," in turn, would be defined to mean six permitted categories of activities, including, for example, activities necessary to "maintain or analyze the functioning of the website or online service,"

---

[41] *See, e.g.*, *Brown v. Entm't Merchants Ass'n*, 131 S. Ct. 2729, 2735-36 (2011) ("'[M]inors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of protected materials to them.'" (quoting *Erznoznik v. Jacksonville*, 422 U.S. 205, 212–13 (1975))); *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503 (1969) (recognizing that teenagers have a right to express their opinions at school).

[42] *See, e.g.*, *Hooper v. California*, 155 U.S. 648, 657 (1985) ("The elementary rule is that every reasonable construction must be resorted to in order to save a statute from unconstitutionality.").

"authenticate users of, or personalize the content on, the website or online service," and "protect the security or integrity of the user, website, or online service."[43]

As noted above, plugin providers do not operate "on behalf of" the operators of websites on which their plugins appear, and data collected by plugins is used primarily to support the functionality of the service of which the plugin is a part. For example, when a user clicks the "Like" button on a website, the primary function of that click is to display the fact that the user "Liked" the website on his or her Facebook Timeline. And while the website may achieve incidental benefits by having large numbers of people who "Like" it on Facebook, the primary functionality of the "Like" button is not to convey information to the operator of the website or otherwise to facilitate the website's operations.

Accordingly, for the limited cases in which a plugin provider would be an "operator" under COPPA, the Commission should improve the definition of "support for internal operations" by providing clearer guidance in three respects.

1. The Internal Operations Exception Must Apply to Any Individual Operator. The Commission should clarify that where a child-directed site or service integrates a plugin, the proposed definition of "support for internal operations" applies to each party individually to the extent each party is an operator. That is, because a plugin provider operates independently and uses data it collects to offer its service, the "support for internal operations" exception should apply to the service of which the plugin is a part. Likewise, when a website publisher collects data on its own, the "internal operations" should be those of the website publisher.[44] The point of allowing "internal operations" purposes is to enable the provider of those services to "maintain or analyze the functioning of the website or online service," which for the plugin provider, is essential to continued operation and maintenance of its plugins. Failing to recognize that plugins are not simply software operated by website publishers but instances of an entirely distinct service would fundamentally undermine the ability of plugins to function.

Moreover, permitting plugin providers, such as Facebook, to rely on the "support for internal operations" exception would be consistent with users' expectations and plugin providers' practices. Notably, when a user visits a page where a Facebook plugin is integrated, the user knows of Facebook's presence because our iconic plugins (such as the "Like" button) are clearly visible on the page. And consistent with the "support for internal operations" definition, we use the data that we collect through plugins to personalize content, perform debugging and analytics, troubleshoot, and maintain security on the broader service of which the plugins are a part.

2. Internal Operations Must Include Service Improvements. Facebook supports Microsoft's proposal to amend the definition of "support for internal operations" to explicitly

[43] 77 Fed. Reg. at 46,648.

[44] If the Commission concludes that plugin providers are "operators" or "co-operators" with respect to the websites and online services in which their plugins are used—a conclusion that Facebook does not support—it should conclude that "internal operations" applies to both the plugin service and the website on which the plugin appears. It would be inconsistent and arbitrary for the Commission to conclude that plugin providers are "operators" for the purpose of liability but not for the exception that enables data to be used to provide requested services.

cover site and service improvements.[45] We understand that the "site maintenance and analysis" category extends to activities that improve the website or online service (which includes site and service improvements), and we urge the Commission to make this point very clear. In addition to using plugin data to facilitate engagement with and personalization of websites, we use data that we receive from our social plugins on an aggregated basis to understand and improve our plugins—for example, to learn how people use the plugins and to speed up the user experience. These improvements help us "maintain" the functioning of Facebook by continuing to improve its functionality over time.

Significantly, the Commission concluded in its 2012 privacy report that (1) certain types of product improvements should be considered "internal operations" that are consistent with the context of the user's interaction with the business, and (2) because these types of product improvements are accepted and expected, less stringent safeguards are needed to protect consumer privacy.[46] The Commission should maintain consistency with that analysis in the COPPA Rule by concluding that COPPA-covered operators may use persistent identifiers to make site and service improvements. Children and parents alike expect online services to continually make improvements in the service offerings available to children. The Commission should make this point explicit by adding the phrase "or develop" after "maintain or analyze" to ensure that operators are permitted to innovate and keep improving their services.

3. Internal Operations Must Include First-Party Advertising. The definition of "support for internal operations" should more explicitly cover first-party advertising. The proposed definition appropriately recognizes that operators should be permitted to engage in first-party advertising. As the Commission acknowledged in its 2009 staff report on behavioral advertising and its 2012 privacy report, the use of context (*i.e.*, the page on which an advertisement appears) and first-party data (*i.e.*, information that a user intentionally allowed an entity to collect directly) in advertising is an expected part of websites and online services that are offered without charge to users, and does not raise the same privacy concerns as third-party behaviorally targeted advertising.[47] The Commission emphasized in its report that it is generally consistent with the context of an interaction for a company to use data collected during first-party interactions for marketing purposes. It then distinguished marketing based on data collected as a third party, which the Commission argued was outside of the generally understood context of a consumer's interaction.[48] The Commission should make that understanding explicit in the COPPA Rule by expressly including first-party advertising under the "internal operations" rubric. This clarification further supports the balance created between the

[45] *See* Microsoft Corp., In re COPPA Rule Review 16 (Dec. 22, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00326-82245.pdf.

[46] *See* FTC, Protecting Consumer Privacy in an Era of Rapid Change 39-40 (2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf (noting that "internal operations" is one of the practices that "would not typically require consumer choice" and specifying that "product improvements such as a website redesign or a safety improvement would be the type of 'internal operation' that is generally consistent with the context of the interaction").

[47] *Id.* at 15-16.

[48] *Id.* at 40-41.

significant demand for free, advertising-supported services, and the expected tailoring of those services.

To reflect these points, the definition of "support for internal operations" should be revised as follows:

> *Support for the internal operations of the Web site or online service* means those activities necessary to: (a) maintain, ~~or~~ analyze, or develop the functioning of the Web site or online service; (b) perform network communications; (c) authenticate users of, or personalize the content on, the Web site or online service; (d) serve contextual advertising or first-party advertising on the Web site or online service; (e) protect the security or integrity of the user, Web site, or online service; or (f) fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4); so long as the information collected for the activities listed in (a)-(f) is not used or disclosed to contact a specific individual or for any other purpose. For purposes of this definition, Web site or online service includes the Web site or online service that collected the information, as well as any operator on whose behalf the information is collected or maintained.

III. The Commission Should Not Undermine Its Stated Goal of Encouraging Cooperation Between Website Publishers and Plugin and Application Providers by Imposing Excessive and Unnecessary Burdens on Parents.

The Commission correctly recognized in the SNRPM that plugin providers typically do not have a direct relationship with the operators of websites and services on which their plugins appear. This makes it impracticable for the plugin provider to evaluate the content of, or police the data practices of, those websites and services, let alone take responsibility for managing the notice and consent obligations of those operators. However, the SNPRM also expressed the Commission's broader goal of encouraging operators of websites and their partners to "cooperate to meet their statutory duty to notify parents and obtain parental consent."[49]

Facebook agrees with the Commission that it is important to encourage entities to cooperate in satisfying COPPA obligations, particularly when this cooperation can result in simplified notices that parents can better understand and make it easier for parents to manage requests for consent from various websites and services accessed by their children. Under the revised COPPA Rule, the Commission would make it more difficult for entities to cooperate and provide rich and interactive services to children. However, with some further revisions, the Commission can promote cooperation between entities that provide robust services to children through a single platform, which will advance the goals of COPPA.[50]

[49] 77 Fed. Reg. at 46,645.

[50] As noted above, in enacting COPPA, Congress sought to achieve several distinct but complementary goals, including "to enhance parental involvement in a child's online activities in order to protect the privacy of children

A. The Commission Should Clarify the COPPA Rule to Promote Cooperation Between Sites or Services and Third-Party Services in Order to Encourage the Offering of Rich, Innovative Services to Children Under 13.

Facebook is concerned that—in addition to the increased burdens on operators themselves—the proposed expansion of the scope of the COPPA Rule could make it harder for parents to understand the most important information: how their children's data will be collected and used by operators of websites and online services their children use. In short, the proposal could make it harder for parents to exercise meaningful control over their children's information.

While Facebook disagrees with the SNPRM's proposed imposition of liability on plugin providers, given those providers' limited ability to meaningfully impact website publishers' practices, there are other ways by which the Commission could more effectively promote the goal of increasing cooperation to the benefit of parents and their children. Specifically, the Commission could retain the multiple operator exception and add an explicit clarification that operators can use a common mechanism, such as one provided by a platform in which multiple operators participate, to provide notice and obtain verifiable parental consent.[51] This voluntary approach would advance COPPA's aim of enhancing parents' ability to understand, control, and supervise their children's online activities.

The concept of enabling one entity to obtain consent on behalf of operators that use its platform was suggested by a number of commenters—including ACT, CCIA, FPF, Microsoft, SIIA, and Disney—in the 2011 rulemaking proceeding.[52] The commenters suggested that a platform provider should be able to provide general notice and obtain parental consent on behalf of app developers and other third parties that utilize the platform to collect personal information for purposes that are specified in the general notice. Under this proposal, only app developers who want to handle information in ways that differ from the general notice provided by the platform would need to independently provide notice and obtain verifiable consent.

---

in the online environment" *and* to "preserve[] the interactivity of children's experience on the Internet and . . . children's access to information in this rich and valuable medium." 144 Cong. Rec. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan).

[51] The Commission is authorized to adopt new consent methods without issuing another SNPRM. The September 2011 NPRM advised that the Commission was considering eliminating the multiple-operator provision, and a number of commenters responded by proposing a platform consent model. Therefore, there has been ample notice and public discussion of possible revisions to the process of providing notice in scenarios where multiple operators offer services through a single user interface. The concept of cooperative consent is also a reasonable outgrowth of the SNPRM's recognition that independent parties who jointly provide services can be deemed "co-operators" who share responsibility for notifying parents and obtaining consent under the Rule.

[52] Ass'n for Competitive Technology, Reply Comments on COPPA Rule Review 7-8 (Dec. 23, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00355-82382.pdf; Comment of Computer and Communications Industry Ass'n, In re COPPA Rule Review 6-8 (Dec. 23, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00358-82384.pdf; Future of Privacy Forum, In re COPPA Rule Review 5-6 (Dec. 22, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00316-82219.pdf; Microsoft Corp., In re COPPA Rule Review 14 (Dec. 21, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00326-82245.pdf; Software & Information Industry Ass'n, In re COPPA Rule Review 10-12 (Dec. 23, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00363-82389.pdf; Walt Disney Co., In re COPPA Rule Review 18 (Dec. 23, 2011), http://www.ftc.gov/os/comments/copparulereview2011/00368-82393.pdf.

Facebook agrees that operators should be permitted to coordinate with a platform provider to provide notice and obtain verifiable parental consent on behalf of themselves and other operators that collect, use, and disclose the child's personal information in ways consistent with the notice provided to parents. Operators also might be able to engage platform providers to facilitate other COPPA obligations, such as providing parental access to data collected by operators. In our view, this concept should encompass scenarios in which a platform provider obtains verifiable parental consent or fulfills other COPPA functions on behalf of app developers, as well as scenarios in which website publishers serve a similar role on behalf of other entities that collect information through their websites. A rule that enables operators to leverage a common platform to provide notice to, and obtain verifiable consent from, parents would substantially advance the Commission's goal of ensuring that clear information is available to parents in a manner that they can easily understand and manage.

B. The Act of Providing Notice and Consent Services to Operators Should Not Transfer the Operators' Liability Under COPPA to the Platform Provider, Nor Does It Turn the Platform Provider into a "Co-operator" of the Underlying Service.

Of course, the fact that an operator used the services of a platform provider to deliver notice to parents and obtain verifiable parental consent should not change the operator's legal responsibility to act consistently with the substance of the notice. In order to ensure that platform providers have the ability to serve in this important role, the Commission should clarify that the act of providing notice and consent services to operators does not, in turn, transfer the operator's *liability* under COPPA from the operator to the platform provider, nor does it turn the platform provider into a "co-operator" of the underlying service. This clarification is critical to ensuring that platform providers are not deterred from helping parents to consolidate notices and consents because of the prospect that they might take on liability for the practices of independent operators that use their services.

This policy is well-established in other areas of law, where regulators acknowledge that an entity without primary regulatory obligations may nonetheless be in a position to promote regulatory goals. For example, the policies underlying Section 230 of the Communications Decency Act and the safe harbor provisions of the Digital Millennium Copyright Act both protect Internet service providers from liability if they transmit a communication that, for example, is alleged to be defamatory or to violate copyright.[53] In adopting these policies, Congress recognized that Internet service providers play a valuable role in connecting two parties to a communication, which the parties themselves could not as easily accomplish on their own. It also recognized that Internet service providers would be unable to continue to provide connectivity services if the act of doing so created virtually unlimited liability for the acts of the entities that used their services to communicate.[54]

---

[53] *See* 47 U.S.C. § 230; 17 U.S.C. § 512.

[54] Similarly, the Federal Communications Commission's new closed captioning requirements for video programming delivered online provide another example of an agency apportioning liability based on different entities' respective roles in the online ecosystem. The FCC recognized that "video programming owners" (*e.g.*, a copyright owner of a television program) have the primary obligation to caption programming and to inform video programming distributors about which video programming needs to be captioned, using a mechanism that the parties agree upon. Video programming distributors and providers may rely on a certification from the video programming owner that programming need not be captioned and, as long as the video programming distributor or provider renders or passes through closed captions and makes a good-faith effort to identify programming that must be captioned, it is protected from liability for distributing programming without closed captions or that has

C. Permitting Cooperative Consent Could Dramatically Improve Parents' Ability to Manage Their Children's Data Sharing While Substantially Reducing Compliance Burdens for Operators.

Consistent with these examples, Facebook believes that modifying the COPPA Rule as described above and in the 2011 comments would minimize the burden and cost on parents in several important respects. *First*, it would eliminate the risk of overly long, overly detailed privacy notices. Instead, parents would receive a general notice up front and then a more specific notice at the time most relevant to the parent—*i.e.*, when the child first wants to use, play, or install an online service available through the interface. *Second*, it would allow the parent to provide verifiable parental consent, consistent with the generally applicable standard in the COPPA Rule, and to exercise ongoing choice over how his or her child's personal information is collected, used, or disclosed by each operator. *Third*, it would minimize the practical cost for parents of providing consent multiple times. For example, without a cooperative consent model, if multiple operators use the credit card method to obtain parental consent, parents may end up being charged multiple fees for their children to use apps available through a single platform.

* * *

We appreciate the opportunity to comment on the SNPRM and look forward to continuing our productive dialogue with the Commission regarding these important issues.

Respectfully submitted,

Erin M. Egan
Chief Privacy Officer, Policy
Facebook

---

captions that are inadequate in quality. Under the FCC's captioning rules, the distributor—which serves a valuable role in delivering television programming to viewers—will not be held liable for captioning failures if the video programming owner was at fault. *See generally* 47 C.F.R. § 79.4.

The Commission's CAN-SPAM Rule, which holds all senders of a commercial e-mail message responsible if a designated sender fails to comply with the substantive requirements of the statute, is inapposite here. Unlike in the e-mail scenario, where there typically are only two or three senders of a single commercial e-mail message, hundreds or thousands of operators may collect personal information through a single online platform. In addition, senders of commercial e-mail are in a much better position to control the designated sender's actions via contract.

APPENDIX

In Section 312.2 of the COPPA Rule, the Commission should modify the proposed proviso in the definition of "operator" as follows:

> Personal Information is *collected or maintained on behalf of* an operator where it is collected ~~in the interest of, as~~ by a representative or agent of~~, or for the benefit of,~~ the operator.

Additionally, in Section 312.2 of the COPPA Rule, the Commission should refrain from adding the proposed paragraph (d) in the definition of "Web site or online service directed to children" and instead add the following proviso:

> *Web site or online service directed to children* means a commercial Web site or online service, or portion thereof, that:
>
> . . .
>
> ~~(d) knows or has reason to know that it is collecting personal information through any Web site or online service covered under paragraphs (a)-(c).~~
>
> . . .
>
> A commercial Web site or online service, or a portion thereof, shall not be deemed directed to children solely because it provides technology to a commercial Web site or online service directed to children, unless the Web site or online service providing the technology is itself directed to children.

Section 312.2 of the COPPA Rule, the definition of "support for internal operations," should be revised as follows:

> *Support for the internal operations of the Web site or online service* means those activities necessary to: (a) maintain, ~~or~~ analyze, or develop the functioning of the Web site or online service; (b) perform network communications; (c) authenticate users of, or personalize the content on, the Web site or online service; (d) serve contextual advertising or first-party advertising on the Web site or online service; (e) protect the security or integrity of the user, Web site, or online service; or (f) fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4); so long as the information collected for the activities listed in (a)-(f) is not used or disclosed to contact a specific individual or for any other purpose. For purposes of this definition, Web site or online service includes the Web site or online service that collected the information, as well as any operator on whose behalf the information is collected or maintained.