September 24, 2012

Hon. Donald S. Clark
Federal Trade Commission
Office of the Secretary, Room H-135 (Annex E)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Via electronic filing: https://public.commentworks.com/ftc/2011copparulereview

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

Dear Secretary Clark:

Google is pleased to submit these comments in response to the Federal Trade Commission's ("Commission") proposed amendments to the Children's Online Privacy Protection Rule ("COPPA Rule") set forth in the Commission's supplemental notice of proposed rulemaking published on August 6, 2012 ("SNPRM"). The SNPRM modifies, in some respects, the Commission's initial notice of proposed rulemaking published on September 27, 2011 ("2011 NPRM").

Google supports the Commission's efforts to protect children online and preserve children's access to appropriate online resources. While Google's products typically are for general audiences and are not directed to children, Google is committed to maintaining a safe and secure online experience for all our users.

Our comments focus on the following points regarding the SNPRM:

- Google believes that the COPPA Rule should neither place compliance responsibilities on third party services that are embedded in sites or services operated by first party entities, nor should first party sites and services be held liable for the practices of independent third parties.

- If the Commission proceeds to place COPPA responsibilities on third party services, it should not impose liability on third parties that do not have actual knowledge that personal information about children under 13 is being collected.

- The Commission should clarify that mobile application platforms would not become "operators" under COPPA by offering apps to the public or reviewing apps for compliance with a platform's technical requirements and terms of use.

- Google is concerned that the practical and technical challenges created by the Commission's cumulative proposed amendments, especially the contemplated new definition of "personal information," will limit operators' ability to sustain and develop legitimate children's offerings.

The Proposed Rule Does Not Provide Clear Guidance and Would Reduce Privacy by Compelling Operators of Embedded Online Services To Collect More "Personal Information"

The Commission's 2011 NPRM would have the effect of applying COPPA to activities – and therefore entities – not previously subject to COPPA. Of particular concern, the 2011 NPRM proposed to extend COPPA requirements to online services embedded into sites and services operated by other entities ("third party embedded" services). Google and other commenters described how this outcome would create unworkable technical difficulties because operators of such third party embedded services do not have the ability to know whether the sites that choose to incorporate their services are directed to children under 13.

In the SNPRM, the Commission has taken a step intended to address this concern. The Commission recognizes in the SNPRM that "the strict liability standard … is unworkable for advertising networks or plug-ins because of the logistical difficulties such services face in controlling or monitoring which sites incorporate their online services."[1] Unfortunately, as explained below, the Commission's new approach to third party embedded services creates unworkable technical challenges and compels such services to collect additional individually identifiable information in order to comply. This is because third party embedded services, including Google's, have been architected and widely deployed in a way that avoids the collection of "personal information" in reliance on the current COPPA Rule.

The cumulative COPPA Rule amendments now proposed will have an unprecedented effect on third party embedded services, bringing many such services under COPPA for the first time even if they are collecting very limited data that is not individually identifiable.

The COPPA Rule Should Not Place New Compliance Responsibilities on Operators of Third Party Embedded Services

Under the current COPPA Rule, the term "website or online service directed to children" is defined as commercial sites or services that are "targeted to children."[2] In determining whether a site or

[1] 77 Fed. Reg. 46, 643, 46,645 (August 6, 2012) (hereinafter "SNPRM").
[2] 16 C.F.R. § 312.2.

service is targeted to children, the Commission looks to factors that relate to characteristics of the site or service that are visible or otherwise evident to users.[3] The operator therefore can generally control whether a site or service is "directed to children" by controlling how it is designed and presented. The terms "directed" and "targeted" in the current Rule have provided important clarity on COPPA liability. A site or service generally does not fall under the definition unless it is *intentionally* developing content for children. Operators currently are obligated to comply with COPPA only when they have actual knowledge that they are collecting or maintaining "personal information" about children.

The SNPRM would expand COPPA liability for first parties that incorporate third party embedded services.[4] First parties should not be liable for third party practices when they do not control the activities of third party embedded services or control or own the data collected by such services. Google is concerned that this broad interpretation of the statute's application to practices "on behalf of" an operator will inhibit first parties from incorporating third party services, thereby undermining operators' ability to offer free or low-cost children's resources. Instead, the Commission should maintain its longstanding position that data "ownership" and "control" determine whether an entity is an "operator" under COPPA.

In addition, the SNPRM would dramatically expand the scope of COPPA by explicitly bringing third party embedded services under COPPA if a service "knows or has reason to know that it is collecting personal information through any website or online service" that is subject to COPPA. This would be true even where the third party embedded services – such as YouTube – are providing functionality in a privacy-sensitive way that collects no individually identifiable information from users. Embedded services, by definition, do not have any ability to control the factors that determine whether a site or service is "directed to children." Likewise, there is no feasible way for third party embedded services to understand when COPPA obligations are triggered based on activities that are occurring on third party websites.

Moreover, many third party embedded services have been architected in a way that acknowledges the bright line – reflected in the COPPA statute itself and in the current COPPA Rule's definition of "personal information" – between individually identifiable information and non-individually identifiable information. In blurring this line, the SNPRM would create enormous disruption to third party embedded services and the websites that have utilized them in reliance on the bright line drawn by the COPPA statute and the current COPPA Rule. Ironically, third party embedded services that collect only non-individually identifiable information would need to collect additional information in order to comply with COPPA's notice and consent requirements.

Unlike the sites and services they support, third party embedded services in such circumstances generally do not have direct relationships with consumers. Indeed, part of the value of embedded services lies in seamless integration with the site or service that is directed to consumers. Consumers

---

[3] *Id.*
[4] SNPRM at 46,644.

may be confused or even suspicious if they are solicited to provide individually identifiable data by a third party embedded service, especially in light of growing awareness about "phishing" threats. The Commission advises consumers: "If you get an email or pop-up message that asks for personal or financial information, do not reply."[5]

For these reasons, Google believes that the COPPA Rule should continue to place compliance responsibilities on site operators and not third party embedded services.

The "Reason to Know" Standard Does Not Provide Clear Guidance

If the Commission retains COPPA liability for third party embedded services in any final Rule, Google encourages the Commission to delete the "reason to know" element of its proposed liability standard. We are concerned that the "reason to know" standard will create considerable uncertainty and compliance challenges for third party embedded services.

In its commentary on this provision, the Commission explains that there would not be a duty for third party embedded services to "monitor or investigate whether their services are incorporated into child-directed properties" but that operators may be exposed to liability if "credible information" is "brought to their attention" that they are collecting "personal information" from another site or service that is directed to children.[6] Google supports the Commission's view that third party operators should not have a duty to monitor or investigate. In other respects, however, this commentary provides scant practical guidance on what constitutes an actionable "reason to know" that another site or service is "directed to children." Furthermore, a "reason to know" standard demands fact-specific analyses, making it extremely difficult for operators to craft effective compliance strategies in advance.

The Commission's introduction of a "reason to know" standard also departs from the liability standards defined in the COPPA statute. COPPA provides that a site or service can be liable only if it is directed to children or has actual knowledge that it is collecting personal information from a child.[7] The SNPRM proposes to qualify the "directed to children" element of this test by incorporating a "reason to know" standard that applies only to third party embedded services.

In its 2011 NPRM, which reaffirmed COPPA's "actual knowledge" standard, the Commission pointed out that an actual knowledge standard is "far more workable, and provides greater certainty" than other legal standards, and that adoption of a lesser standard "might require operators to ferret through a host of circumstantial information" to determine if COPPA applies.[8] The same persuasive objections apply to the Commission's effort to insert a "reason to know" standard into the "directed to children" prong of COPPA.

---

[5] Federal Trade Commission, "How Not To Get Hooked by a 'Phishing' Scam," available at http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm.
[6] SNPRM at 46,645.
[7] 15 U.S.C. § 6502(a)(1).
[8] 76 Fed. Reg. 59,804, 59,806 (Sept. 27, 2011).

The Proposed Definition of "Personal Information" Would Reduce Privacy by Compelling Operators of Embedded Online Services To Collect More Data To Comply with COPPA

The challenges discussed above primarily stem from the Commission's proposal to expand "personal information" under COPPA to a variety of data elements that do not permit individual identification or contact. Google continues to believe, as detailed in our prior comments, that the Commission's proposed expansion of "personal information" would require significant changes in the way that third party embedded services are delivered, especially if the final Rule does not address the concerns above.

The SNPRM would define as "personal information" any persistent identifier that "can be used to recognize a user over time, or across different Web sites or online services," regardless of whether an identifier is functionally used in this way.[9] The Commission's list of persistent identifiers makes clear that this definition includes the range of technologies – such as IP addresses, random identifiers in cookies, and device identifiers – that are widely used today to deliver services without collecting individually identifiable information about users. The new definition could potentially also bring device manufacturers within the definition of an "operator" because they create and use device identifiers for service purposes. It is not clear that these practices are protected under the "support for internal operations" exception, and manufacturers face the additional concern that they cannot control other entities' use of such identifiers.

Google, like other companies, relies on persistent identifiers to offer privacy-sensitive services and tools that avoid the need to have users sign in or otherwise provide individually identifiable information. Under the SNPRM, such services will be in an unworkable position: the data collected will be sufficient to trigger COPPA liability, but not sufficient on its own to comply with COPPA. Companies cannot send a direct notice to, or rely on consent from, an IP address alone. The SNPRM, like the NPRM, would therefore create a perverse incentive for operators of such services to collect and maintain additional and more personal data for children and parents in order to satisfy the Commission's new COPPA Rule. Indeed, sites and services that have prioritized privacy to date would effectively be penalized for their privacy-sensitive approach because they would face a disproportionate compliance burden in transitioning to the new regime. By the same token, the proposed approach would eliminate current incentives for sites and services to work with third party embedded services that are privacy sensitive (*i.e.*, do not collect individually identifiable information or contact information).

The parental access and deletion rights generally required under COPPA would pose a particular challenge for providers of embedded third party services. Google offers users granular tools for control in connection with online advertising. Even these tools, however, do not necessarily provide access to persistent identifiers in situations where Google cannot authenticate a user. The proposed changes to the COPPA Rule would nevertheless require access to this data, despite the fact that

[9] SNPRM at 46,652.

access would be largely meaningless to parents. This proposal also raises serious security concerns about appropriate authentication procedures for unauthenticated individuals that might seek to exercise data access and deletion rights under COPPA.

In the mobile app ecosystem, likewise, third party services that are incorporated into mobile apps do not have the technical capability to deliver "push" notices, prompts, or other user interfaces that could enable COPPA compliance without cooperation from the first party app developer. For security reasons, mobile operating systems are designed to prevent such third party practices. Third parties therefore would be reliant on first parties to incorporate code that could enable COPPA compliance.

The implementation concerns discussed above make the "support for internal operations" exception critically important. Google appreciates the Commission's effort to revise this exception in response to prior comments and believes this revision is a step in the right direction, but the exception remains underinclusive. Other legitimate and valuable practices involving persistent identifiers (not individually identifiable information or contact data) seemingly fall outside this exception, and therefore would be brought within COPPA for the first time under the SNPRM.

As one example, Google offers a tool for embedding YouTube videos within websites that does not require users to register with YouTube or otherwise provide individually identifiable information to Google. The tool utilizes the IP address and a browser cookie to keep track of how many unique viewers have accessed the video from any website. (Note that while these technologies would be "persistent identifiers" because they "can be" used across websites, this tool uses them only within a single website.) In the aggregate, this data is important both to the user who uploaded the video and to advertisers and content developers. While we view this analytics activity as a form of "internal support," it is unclear whether this would be covered by the SNPRM's proposed definition.

Other routine practices would be in a similarly uncertain position under the Commission's proposed exception. The SNPRM's framework thus creates exposure not only for third party services but also for sites and services that may incorporate them.

The Commission Should Clarify that Mobile Application Platforms Would Not Be "Operators" Under COPPA

The Commission's revised definition of an "operator" would create unique compliance challenges for Google Play and other platforms for mobile applications that would be exacerbated by the "reason to know" standard. Google Play is an open platform that enables any developer to offer an application to any user with a mobile device running on the Android operating system. There are currently over 600,000 applications on Google Play. In any given month, tens of thousands of new apps are made available to users on Google Play. Google suggests that the Commission clarify that neither a platform's offering of an app to the public nor a platform's process for reviewing apps for compliance with the platform's technical requirements or terms of use would transform the platform

into a COPPA operator or provide the platform or a platform's affiliates with knowledge or a "reason to know" of an app's COPPA status.

First, a mobile application platform should not be considered "directed to children" solely because it offers public access to child-directed apps. Google Play and other mobile application platforms do not control the practices of unrelated app providers and should not face liability based on such practices.

Second, imputing the "know or have reason to know" standard to a mobile application platform would create profound challenges for mobile application platforms. The sheer volume of apps that are offered on these platforms on a daily basis makes it impossible for them to oversee or administer any COPPA-related classification of apps that might be required under the SNPRM. The test for determining whether a site or service is "directed to children" involves a close legal and factual review of numerous factors. Platform posting and review procedures are not designed, and cannot feasibly be designed, to conduct this type of analysis.

Google encourages the Commission to avoid creating any liability risk that will compel platforms to stop providing access to apps that could be considered child-directed. We believe the best way to address this concern is to eliminate the "reason to know" element of the definition, clarify explicitly that app platforms would not ordinarily "know" whether an app that is submitted to or offered on the platform is "directed to children," and clarify that the definition of an "operator" does not encompass platforms that merely make third-party apps accessible to users for download.

The Proposed Rule Could Reduce Online Offerings for Children

In response to the Commission's initial NPRM, Google and other commenters highlighted numerous difficulties that would arise from the Commission's proposals. Google appreciates the Commission's efforts to address certain of these challenges through the modifications put forward in the SNPRM. Nevertheless, as detailed above, significant concerns remain including the fact that many third party embedded services would need to begin collecting individually identifiable information to comply with COPPA. Google is concerned that these challenges would force operators of children's online resources to make an unappealing choice between eliminating third party services from their sites and services, or complying with COPPA on behalf of those services – even if a service's data collection is limited, for example, to a single cookie with a random numeric identifier. In many cases, sites and services may not currently be collecting "personal information" on their own behalf, and would have to begin collecting personal information from children in order to meet COPPA requirements.

We are concerned that these challenges will undermine the ability of sites and services to provide engaging online resources to children. COPPA should not become a barrier to children's ability to access appropriate and beneficial online resources for education and entertainment. Small publishers and app developers that are more reliant on third party embedded services, and do not

have the capacity to develop in-house alternatives, are likely to be impacted most severely. As an initial matter, eliminating third party embedded services could make children's offerings less interactive and exciting, especially in contrast to services that are available elsewhere online. Children could turn to resources that are not age-appropriate or other non-COPPA-compliant resources in search of more interactivity.

Inhibiting sites and services from incorporating third party embedded services could cut off access to advertising revenue and make it more difficult to operate resources for children. A significant majority of Google's millions of online advertising customers are small businesses. Online advertising supports the rich array of online content and educational resources that these and other publishers provide to children, often at low or no cost. Many companies do not have the capacity to develop comparable advertising tools and are unlikely to succeed under a paid-registration model. The SNPRM raises the additional concern that these impacts will affect even mixed-audience sites and services that fall within the proposed "disproportionately large" audience standard. Google encourages the Commission to investigate and consider the impact of its SNPRM proposals on publishers of all sizes, and to consider mitigating these impacts as suggested above.

* * *

Thank you for the opportunity to provide comments on the Commission's SNPRM and its likely effect on the online ecosystem. We look forward to continuing to work with the Commission in pursuit of a safe and secure online environment for all users including children. Please contact me with any questions by email at or by phone at

Sincerely,

Pablo L. Chavez
Director of Public Policy
Google Inc.