December 23, 2011

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 proposed amendments to the Children's Online Privacy Protection Act Rule.

We appreciate the Commission's continued attention to children's online privacy, and share its deep commitment to protecting the privacy and safety of everyone, including children, in their online activities.

While Google's products are for general audiences and are not directed at children, maintaining a safe and secure online experience for everyone is a fundamental part of our responsibility to our users. We also recognize that our business depends on maintaining our users' trust in the Internet and in our products. Google is committed to ensuring that all users stay safe and enjoy appropriate privacy protections online, and we support this important objective underlying the COPPA framework. Younger Internet users and their parents must also have an abundance of appropriate content and services to enjoy online, and the knowledge and skills necessary to stay safe while they enjoy them. Google is committed to increasing this "digital literacy"—the life skills of the 21st Century—for all consumers.

In our comments, we will describe how Google has worked to advance the COPPA goal of a safe and secure online experience for children and all users, and how the Commission's proposed amendments to the COPPA Rule (the "Proposed Rule") would affect that goal. In particular, we highlight the following points:

- Regardless of the precise contours of the regulatory framework, children's online privacy must be advanced foremost by empowering parents with tools to make choices about their families'

online experiences and by increasing digital literacy. For our part, Google offers industry-leading filtering tools, such as SafeSearch and YouTube Safety Mode, that enable parents to better guide their children's online activity, and educates families about protecting their online privacy and safety through projects such as the Google Family Safety Center and Good to Know websites.

- We share the Commission's goal of increasing the amount and quality of general audience and child-directed online content. The Commission should consider how to alleviate the technical challenges presented by the Proposed Rule that could affect this goal, particularly with respect to smaller publishers that depend on third-party services to offer their content.

- The proposed expansion of "personal information" in the Proposed Rule would significantly alter the current manner of delivery of many online services and advertising. In considering this change, we urge the Commission to avoid creating a requirement that service providers collect additional and more sensitive information about children and their parents.

I. Google's Approach to Protecting the Safety and Privacy of Our Users Including Children

The Internet offers tremendous opportunities to enrich children's lives by offering innovative new resources for education, self-expression, and collaboration. For example, millions of students of all ages receive homework help from the Khan Academy, a non-profit organization that uses Google's YouTube platform to share educational videos on topics ranging from basic arithmetic to vector calculus. At the same time that the Internet enables these types of enriching opportunities, it also presents challenges in ensuring that youth have an age-appropriate experience online.

Google believes that empowering parents with tools to manage their family's online activities and equipping everyone with digital literacy skills should be the cornerstone of efforts to protect children's privacy and safety online. Consistent with this philosophy, we have invested significant resources in a three-pronged approach to children's online privacy and safety: (a) developing tools to empower parents and other users to protect their family's privacy and safety, (b) providing educational initiatives to promote family and child awareness, and (c) collaborating with industry and law enforcement partners on additional safety initiatives to protect children.

Through a range of initiatives, discussed further below, we help children and parents take steps to protect their privacy and safety online, while also enjoying the Internet's rich array of resources.

A. Safety Tools

The open and participatory nature of online resources creates extraordinary richness, but also presents the possibility that children may encounter inappropriate content or engage in inappropriate sharing online. Consistent with COPPA's emphasis on engaging parents in children's online experiences and ensuring privacy protections appropriate for children, Google has developed technical tools that empower users to protect their online safety as individuals and as a user community.

1. *Content Filters*

Google services include filtering tools that users can implement to control objectionable content. In keeping with our emphasis on user participation, the filters are implemented through a combination of automated review and user flagging.

SafeSearch and SafeSearch Lock

For our web search product, Google has developed a SafeSearch feature that parents can use to filter sexually explicit images and text in search results. This feature enables parents and other concerned users to block searches from returning adult sites or explicit content. SafeSearch is also available on mobile devices.

Setting SafeSearch

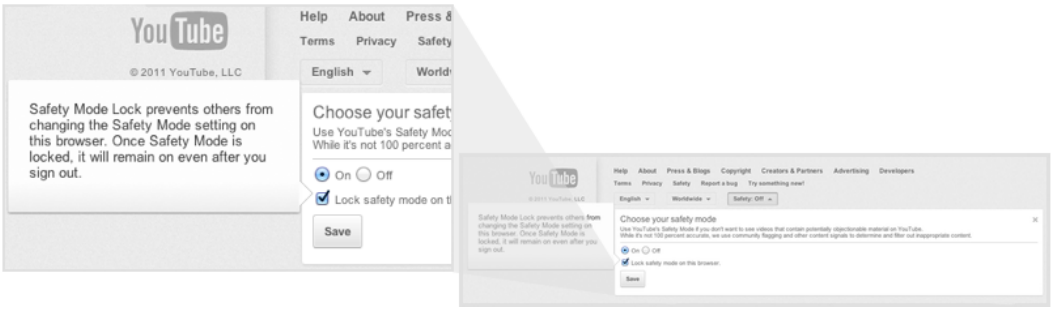
The tool also offers a SafeSearch Lock option to allow users to lock a computer's SafeSearch setting to the strict filtering level. Once the SafeSearch filtering level has been set, the level cannot be changed without a password. Parents can observe whether the feature is on, even from across a room, because the feature displays colored balls across the top of the monitor screen when the setting is locked.

SafeSearch when locked

YouTube's Safety Mode

YouTube, a video sharing website owned by Google, includes a Safety Mode setting that is designed to allow users to exercise control in order to avoid being exposed to potentially objectionable content. The blocking list for this feature is identified through a combination of automated screening and community feedback.

When Safety Mode is turned on, the feature prevents videos with potentially objectionable content and videos that have been restricted to users 18 and older from displaying in video search, related videos, playlists, shows, and movies. The feature blocks content that is permitted under YouTube's policies, but may not be appropriate for all users. Parents may select this Safety Mode by clicking on the link at the bottom of any video page and may lock the setting on the browser using an account password.



Safety Mode: signed in

2. *Community Guidelines and Ratings*

Google also sets community guidelines for our services, and provides users with reporting tools as an effective and efficient means to enforce such guidelines.

Community Reporting

Many of Google's online offerings facilitate user participation in enforcing product rules. We enable users to maintain community standards with reporting tools that allow users to report various kinds of content that may be objectionable including violence, mature content, hate speech, promotion of illegal conduct, spam, or other violations of Google's content policies. These tools are available for our popular services that rely on user-generated content, such as YouTube, Picasa Web Albums and Blogger.

Reporting tool

Android Market Ratings

Android is Google's open source mobile platform, for which any developer can create applications, commonly known as apps. Google's Android Market provides one source from which users can obtain such apps. Although not specifically designed as a parental control, Android Market contains a content rating system that requires developers to rate their apps in one of four categories: Everyone, Low Maturity, Medium Maturity, or High Maturity. We have established guidelines that require minimum ratings for apps that contain content some might find objectionable or that enable direct communication with other users. A PIN code can then be used to lock a device to its chosen setting. Choosing a setting will filter apps so that only apps within the selected maturity level can be displayed and downloaded to the device.

Google takes corrective action against those apps and developers in Android Market whose ratings do not conform to our rules. Users help enforce the content rating system by flagging apps for review. Google evaluates apps flagged for ratings violations according to our guidelines, and takes action to force a ratings change or remove apps that violate the guidelines.

B. Educational Initiatives

The FTC has recognized that educating consumers about how to safeguard their privacy online is a "crucial complement" to COPPA law enforcement activities,[1] and has made important investments in innovative consumer education resources such as the recent NetCetera campaign and toolkit, Admongo.gov, and a host of other publications and interactive tools.

[1] Federal Trade Commission, Implementing the Children's Online Privacy Protection Act: A Report to Congress 19 (2007).

Google shares this commitment to consumer education. We work hard to promote digital literacy among our users, and especially to educate families about how to use the Internet responsibly. Key educational sources that are specific to our products and services include:

- Google's Family Safety Center is a central resource for families to understand Google's child safety tools, report concerns about user-generated content, and obtain online safety tips from Google and child safety organizations. This content supplements information about safeguarding user privacy and security that's available through Google's Privacy Center and Security Center.

- Other Google educational resources include Good to Know, a recent consumer education campaign to provide users with a one-stop-shop for practical guidance on how to safely and securely use online services, and TeachParentsTech.org, which allows users to send tech support videos made by Googlers to family and friends.

- Additionally, Google maintains blog posts, safety guides, and readily-accessible help pages for specific services that provide additional resources. For example, YouTube offers a Safety Center and Parent and Educator Resources pages with information about our tools and tips for staying safe online including advice on keeping personal videos private, protecting online identities, and appropriately managing interactions with other users. In addition, the YouTube Safety Center channel includes a series of digital citizenship and online safety videos including clips on "Playing and Staying Safe Online," "Detecting Lies and Staying True," "Staying Safe on YouTube," and "Steering Clear of Cyber Tricks."

- Google also uses its platforms to highlight resources offered by others on Internet safety. For instance, Google's Public Policy Blog drew attention to Admongo, the Commission's interactive game for children to learn about ads and commercial messages. YouTube has partnered with child safety organizations around the world to create channels featuring online safety content including Beatbullying and Childnet. The Family Safety Center features advice for parents from our child safety organization partners.

We also work with many partners that share our commitment to educating families about online safety. Over the last two years, we've worked with the online safety organization iKeepSafe to develop a curriculum for students about digital literacy and citizenship, and launch a Digital Literacy Tour. The curriculum, which is available online at no cost, includes a resource booklet, presentations, and animated videos covering topics such as how to recognize online risks, investigate and determine the reliability of websites, and avoid scams. Google is conducting a nationwide tour to promote the use of this curriculum in schools. To complement these classroom efforts, we are training parents, teachers, and volunteers to host future workshops and providing advice on how to talk to children about best practices for going online.

In addition to iKeepSafe, we partner with a number of groups to advance online safety including the Family Online Safety Institute, Common Sense Media, Connect Safely, Enough is Enough, GetNetWise,

and Wired Safety. Google works with our partners to solicit feedback and recommendations on our efforts to promote children's online safety, and boost awareness of our granular parental controls. Their feedback has also helped us to build children's privacy and safety considerations into our products before they are released.

C. Law Enforcement and Industry Collaboration to Protect Users

As reflected in the congressional record, the passage of COPPA was motivated by a goal of protecting children from online contacts that might lead to exploitation or other endangerment.[2]

Toward the same goal, Google builds and maintains strong relationships with law enforcement, industry partners, and other community stakeholders to protect children online and to combat illegal activity. Google actively cooperates with law enforcement and other partners to combat child sexual abuse. When we become aware of child sexual abuse images or child pornography in our search engine results or hosted on our sites, we immediately remove any material to which we have access and report all incidents to law enforcement through the National Center for Missing and Exploited Children. Google engineers have also worked with NCMEC to develop new technical solutions for addressing online child pornography and identifying and locating missing children. Google has made significant donations of hardware and software to support NCMEC's data management capabilities, and recently awarded an additional $1 million grant to NCMEC to support its important mission.

We have also participated in numerous stakeholder efforts over the past several years on Internet safety, such as the PointSmart ClickSafe Task Force, which developed the comprehensive "Recommendations for Best Practices for Online Safety and Literacy" report in 2009.

II. Comments on Proposed Amendments to COPPA Rule

We appreciate the Commission's interest in reviewing the COPPA framework in light of the rapid pace of innovation on the Internet and changes in how families use online technologies.

Google's services are intended for general audiences and not directed at children, but we recognize and share the Commission's deep commitment to ensuring the safety and privacy of children online. Despite our limited experience with COPPA, we appreciate this opportunity to offer our observations about the likely impacts of the Commission's Proposed Rule on Google, the Internet, and consumers of all ages.

A. Technical Challenges Presented by Proposed Rule

We share the Commission's goal of expanding the amount and quality of general audience and child-directed online resources, ensuring that families find a rich array of content online in addition to the tools and educational materials needed to protect their privacy and safety. The Commission should consider how the technical challenges presented by the Proposed Rule would affect this goal, particularly

---

[2] *See, e.g.*, 144 Cong. Rec. S8483 (daily ed. July 17, 1998) (statement of Sen. Bryan).

for smaller publishers that depend on third-party services such as embedded content tools and advertising networks to offer their services.

1. Use of Persistent Identifiers to Deliver Content and Advertising

COPPA defines "personal information" as "individually identifiable information collected online," and grants the Commission authority to expand the statutory examples of "personal information" to include identifiers that permit "the physical or online contacting of a specific individual[.]"[3] The Proposed Rule would expand the definition of "personal information" to "persistent identifiers" such as cookies, IP addresses, and unique device identifiers even if they are not combined with any contact information or individually identifying information.[4] Persistent identifiers use randomly assigned numbers to enable online services to recognize the preferences associated with a particular browser or device that may be shared by multiple users, without requiring personally identifying information about any individual user.

Google offers several advertising services that support publishers in making their rich online content and services available to the public for free or at lower cost. These services include our AdSense program and advertising networks that connect advertisers and publishers including DoubleClick and AdMob. As with most other advertising services, Google's services rely on persistent identifiers rather than personally identifiable information. These identifiers are used for a variety of purposes in delivering advertising campaigns on third party sites including tracking campaign performance, limiting the number of times that users see the same ads, delivering payment, and offering other analytics. We also use cookies to deliver more relevant advertisements based on interest categories associated with a particular browser.[5]

Persistent identifiers are also used by third parties to deliver non-advertising services on websites including small applications or embedded content. For example, YouTube offers a tool to embed video on any website without requiring that users of the site sign in to YouTube or otherwise provide personal information to Google. Instead, Google collects the IP address of a user watching an embedded video playback on a website and places a unique YouTube cookie on the browser. This data allows YouTube to determine the total number of unique viewers and views of a YouTube video on YouTube's own site and on third-party sites that embed that video. The number of unique viewers and views of a YouTube

---

[3] 15 U.S.C. § 6501(8)(F).

[4] Proposed Rule and Request for Comment on the Children's Online Privacy Protection Rule, 76 Fed. Reg. at 59812 (Sept. 27, 2011).

[5] Note that Google enables users to opt out of interest-based advertising. For users that opt out, the word "OPTOUT" is written where a unique cookie ID would otherwise be set on a browser, which means that Google cannot track a specific browser across our ad network. More information about Google's efforts to protect the privacy of our users can be found in our Privacy Center, including a description of our five core privacy principles focused on transparency, choice, and security, and initiatives such as our Ads Preferences Manager, which allows users to see and change the interest categories associated with a specific device for advertising purposes and set their opt-out preferences as described above.

video is critical data for both users uploading videos to YouTube and advertisers. Without this data, YouTube would not be able to accurately determine payments to its partners or perform other analytics.

2. Technical Challenges

In expanding the scope of COPPA to include "persistent identifiers" in the definition of personal information, the Proposed Rule may pose significant technical compliance challenges for third party services. While we recognize that the inclusion of the "support for the internal operations" exception in the Proposed Rule is an effort to allow for some uses of "persistent identifiers" outside of the COPPA framework, it does not appear that the use of persistent identifiers by third parties would be covered under that exception, as we explain further below.[6]

We ask the Commission to consider the following technical challenges and work with stakeholders to address the goals of COPPA without impeding the delivery of online services.

- *Providers of third party services on websites or in apps, such as advertising, are not in a position to assess whether specific publishers are offering services "directed to children" that trigger COPPA obligations.* For example, DoubleClick, AdSense and AdMob provide advertising to millions of publishers in an automated system and do not control the non-advertising content or the audience of an online service or app. This content is controlled by the publisher and can be updated at any time without notice to an advertiser or service provider.

- *Under the Proposed Rule, even purely contextual advertising by third-party providers on child-directed sites would be impossible without parental consent.* The Proposed Rule includes as covered information "an identifier that links the activities of a child across different Web sites or online services," without exception, and discusses how the IP address of a user from a child-directed website is considered such an identifier.[7] Even purely contextual advertising delivered by third-party ad networks like Google's requires the collection of IP addresses for at least fraud detection and reporting purposes. The Commission makes clear that it does not want to discourage such contextual advertising, so we urge it to review how this language could be revised to allow the use of identifiers across sites by third-party providers in this manner.

- *Providers of third party services generally cannot know when there are multiple users of a website, browser, or app, making it difficult to obtain consent as required under COPPA.* Because the cookies and IP addresses used by providers like Google to serve content are not specific to identified individuals that have logged in with a username and password, there is no means of registering and maintaining a specific user's age or parental consent. Furthermore, if one user of a family

[6] 76 Fed. Reg. at 59812 (stating in its explanation of the proposed definition of "(h) an identifier that links the activities of a child across different Web sites or online services" that ". . . operators such as network advertisers may not claim the collection of persistent identifiers as a technical function under the 'support for internal operations' exemption").

[7] *Id.*

computer or shared network indicated that he or she were under 13, there would be no way to distinguish that user's data from those of the other, older users.

- *The parental access and deletion rights generally required under COPPA would pose a particular challenge for third party advertising and content providers.* Google has led the market in offering users granular transparency and control in connection with online advertising. Even Google's tools, however, do not currently provide access to raw advertising data, identifiers, or IP addresses, which would be largely meaningless to consumers. Moreover, there are unresolved security issues involved. For example, the unauthenticated nature of persistent identifiers like cookie IDs means that a service provider cannot be sure that the parent seeking access to information associated with a persistent identifier is actually the parent of the data subject, as opposed to another user of the browser.

3. Compliance Challenges May Reduce Online Content for Children, Especially From Small Publishers

If left unaddressed, the technical challenges presented in the Proposed Rule will make it difficult for online advertising and other third party services to operate on websites and apps—ultimately reducing support for publishers and developers providing online resources for children. As a significant majority of our millions of advertising customers are small businesses, Google is especially concerned that the Proposed Rule will disadvantage small publishers and app developers relative to larger entities that can construct such services in-house. We encourage the Commission to explore ways to avoid this unwanted and unnecessary outcome.

As the Commission has recognized, online advertising has significant consumer benefits including providing consumers with information about offers that may interest them and offering a major source of revenue supporting the rich variety of online content that consumers have come to value and expect, from messaging services to social networking to news. Above we discussed reasons why implementing the Proposed Rule would pose thorny technical challenges for providers offering services on third party sites. Larger publishers of content directed at children are in a better position to mitigate these compliance challenges by internalizing certain supporting services, such as advertising, rather than outsourcing them. By internalizing these activities, such entities would eliminate the need for additional data collection, notice, or consent for COPPA purposes.

In contrast, smaller publishers and app developers tend to rely on third party service providers for advertising, applications, video, and other services because they lack the efficiencies of scale or technical ability to handle these activities on their own. Although the Proposed Rule would affect all publishers that use such service providers, smaller publishers would be less able to internalize certain activities. In addition, smaller publishers that are not part of a larger corporate family are more likely to be heavily reliant on advertising revenue to support their resources. As a result, COPPA compliance under the Proposed Rule may prove most difficult and expensive for those publishers that are least able to tackle such challenges. We urge the Commission to investigate the impact of the Proposed Rule on smaller publishers and ways the impact can be mitigated without undermining the goals of COPPA.

B. Expansion of the Definition of "Personal Information" May Prompt Greater and More Invasive Data Collection about Children

The technical issues created by extending COPPA's mandates to unauthenticated data like cookie identifiers and IP addresses, discussed above, may cause many providers to collect additional and far more sensitive information about children and their parents simply in order to register and preserve required parental consent. We urge the Commission to consider how it can avoid this outcome.

Persistent identifiers such as those used in browser cookies deserve some manner of privacy protection, but it is neither optimal nor practicable to apply the *same* protections to all data in all contexts. Rather, data protection measures must be calibrated for different types and uses of data and for different settings. Such calibration should reflect the degree of identifiability, linkability, and sensitivity of data in various contexts. [8] Cookies, for instance, can be cleared from browsers at the end of a session, whereas most service providers typically have records for logged-in users.

The Proposed Rule would put cookies and IP addresses in the same category as personal information such as name and email address that clearly meet the statutory requirement of permitting "the physical or online contact of an specific individual."[9] Currently, providers of services directed at children collecting only cookie or IP address data are not required to obtain parental consent. If these data are lumped in with traditional "personal information" under COPPA, however, providers will not have this "light touch" option. Instead, all such services may be required to obtain parental consent to perform common, simple functions that are not strictly "necessary to maintain the technical functioning" of the service, such as using server logs to perform analytics or preserving user settings like language.[10] To obtain parental consent and reliably know to whom that consent applies, sites directed at children will have to abandon less sensitive methods of data analysis and personalization based on unauthenticated unique identifiers like those in cookies and instead require all users to log in.

The situation could be even more difficult for third-party services operating on child-directed websites, such as advertising, analytics, or embedded content. For example, imagine a video service such as YouTube that offers the ability for websites to enhance their content with embedded third-party video, without requiring any personal information from a viewer to determine whether that person is an adult

---

[8] *See* Comments of Google Inc., Preliminary Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers Comments" 8 (Feb. 18, 2011) (discussing how privacy principles apply differently to personal information versus persistent identifiers: "[f]or example, data security is important for all personal data, regardless of type. In contrast, access and correction rights make little sense where a service provider cannot be sure that the user seeking access is the data subject, such as when the data consists of unauthenticated search query logs").

[9] 15 U.S.C. § 6501(8).

[10] 76 Fed. Reg. at 59830 (defining "personal information" to include persistent identifiers used "for functions other than or in addition to support for the internal operations of, or protection of the security or integrity of, the Web site or online service").

or child. The service uses a cookie to determine the total number of unique viewers and views of a YouTube video, but otherwise the user is not known or identified to the video provider. Under the Proposed Rule, if a service directed at children wanted to embed a video on its website, the video provider would have to force the user to log in with a username and password simply to count the unique playbacks of the video on the child-directed website. And since the parent would not be able to identify his child based on a persistent identifier such as an IP address or cookie ID, the video provider would likely need to collect a child's first name as well as a means to contact the parent. As a result, in order to use a simple website, a child user is logging into several services and providing a great deal of new and personal information.

To avoid this outcome, we urge the Commission to seek means of extending appropriate protections to persistent identifiers that avoid treating all data the same, regardless of its linkability to individual users or sensitivity.

C. COPPA Rule Should Support Continued Innovation in Online Parental Consent Mechanisms

Finally, Google encourages the Commission to explore how new technologies could be used to obtain verifiable parental consent under COPPA, while also fostering parental involvement in children's online activities. The COPPA Rule should be designed in a manner that does not burden or impede the consent process so that parents have reasonable options to support their children's use of online resources in a safe way.

In particular, we believe that COPPA must allow companies the flexibility to provide parents with the ease and convenience of online consent mechanisms that do not require offline steps. For example, the Commission should consider how parental controls could be used to provide verifiable parental consent, particularly when the device or service is closely associated with an authenticated subscription. Tools that enable user control over product features and content could be leveraged to provide parents with a means of rendering consent under COPPA, while also deepening their engagement in their children's use of the Internet. Google believes that providing families with tools to manage their experience online, which may go far beyond facilitating the consent required by COPPA, is the most important means of protecting children's privacy and safety.

* * *

Thank you for the opportunity to provide comments on the Commission's current proposals. We look forward to continuing a productive dialogue with the Commission toward our shared goal of protecting children's online privacy and safety. Please contact me with any questions by email at pablochavez@google.com or by phone at 202.346.1237.

Sincerely,

Pablo L. Chavez
Director of Public Policy
Google Inc.