December 22, 2011

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

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

Dear Secretary Clark:

The Future of Privacy Forum (FPF) is a think tank seeking to advance responsible data practices and is supported by leaders in business, education, and consumer advocacy. FPF thanks the Federal Trade Commission (FTC) for providing this opportunity to comment upon the FTC's proposed amendments to the Children's Online Privacy Protection Rule (COPPA Rule or Rule). FPF offers what we believe are unique insights reflecting best practices and developing innovations regarding data privacy, and we hope these insights help shape how the Rule will continue to protect children's privacy in the online marketplace.[1]

We commend the FTC's commitment to protecting the privacy of children in a rapidly developing online marketplace. Among other key issues, we recognize that precise location information can often be personal and we support including location information as personal when it is sufficiently precise and would allow an individual child to be contacted. We also believe that creating behavioral profiles of children based on their web surfing in order to tailor the ads they see across web sites is not appropriate unless there is parental consent. Few, if any, responsible firms do this, and FPF supports the FTC's efforts to ensure that doing so without parental consent violates the Rule.

These comments do not address all the proposed amendments to the Rule. FPF has chosen to focus on amendments affecting those areas that correspond with the organization's specific expertise and experience. In this submission, we address (I) The proposal to modify the definition of "personal information"; (II) the proposed revisions directed to protecting the security, confidentiality and integrity of information collected from children; (III) geolocation issues; (IV) apps and platform issues; and (V) new parental consent mechanisms.

I. Modifying the definition of "personal information."

The FTC proposes to modify the definition of "personal information" in the COPPA Rule because changes in technology and marketing practices have affected the current Rule's ability to regulate the use of

[1] The views herein do not necessarily reflect those of the Advisory Board or supporters of the Future of Privacy Forum.

children's information and the practice of targeting children with behavioral advertising.[2] Under the new, expanded definition, identifiers that link a child's activities across Web sites or online services would be considered personal information.[3] And the same would be true of persistent identifiers, such as cookies or IP addresses, unless those identifiers were used only to support the internal operations of the Web site or online service.[4] The FTC considers these types of information to be personal because they enable operators to contact specific individuals.[5]

The straightforward way to regulate the ability of operators to target children with behavioral advertising would be to simply prohibit operators from engaging in the practice as it has previously been defined by the FTC.[6] But the FTC instead focuses on the types of information operators *collect* rather than on how operators *use* the information.

This approach unnecessarily risks imposing COPPA's notice and consent requirements on those operators who use information in ways that *do not* raise significant privacy concerns. In its discussion of proposed paragraph (g) of the definition of "personal information," the FTC recognizes the validity and significance of such a risk.[7] Because operators must collect certain persistent identifiers (*e.g.*, IP addresses) to provide basic online services, the FTC proposes that those identifiers collected solely to facilitate the internal operations of a Web site or online service should not constitute personal information. Without such an exception, all children's Web sites and online services would be subject to COPPA's requirements. And the FTC acknowledges that this would render the Rule "over-broad and unworkable."[8]

The proposed carve out from the definition of personal information is not broad enough to make the Rule workable. As defined, it would restrict almost all ad serving, ad tracking, analytics and social plug-ins as conducted today.

Operators of web sites and online services for children rely on a range of third parties to sell and deliver advertising. The typical operator does not negotiate with individual advertisers to arrange for the placement of many of the ads on the operator's Web site or online service. Rather, many operators sell advertising space to ad networks that act as intermediaries between operators and advertisers. In turn, ad networks sell advertising space to advertisers and arrange for third party ad servers to deliver ads to users who visit the sites and online services. These ads may be simply targeted to reach the type of audience expected at a particular web site or collection of Web sites, without any reference to previous activity by a child.

Each time an ad is delivered by an ad network on any of the sites it may be serving, a cookie is set or read. This cookie may be used across web sites to count the number of unique viewers of the ad, to frequency cap an ad, or to understand which ad has been successful at bringing users to an advertiser's site. An advertiser purchasing ads on multiple sites will typically use a third party adserver acting on its behalf to serve its creative simply so that it can receive reporting about ad delivery and clicks that is consistent across many sites.

The proposed changes to the rule would treat this collection of non-personal information as personal and thus bring to a halt the basic information collection relied on by advertisers and web publishers for basic understanding of their ad campaigns.

---

[2] *See, e.g.*, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59810–59814 [hereinafter Proposed COPPA Rule] (proposed Sept. 15, 2011), *available at* http://www.ftc.gov/os/2011/09/110915coppa.pdf (proposing changes to the definition of "personal information" under 16 C.F.R. 312.2).
[3] *Id.* at 59812.
[4] *Id.*
[5] *See id.* at 59811.
[6] *See generally* FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising 46 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (defining "behavioral advertising" as "the tracking of a consumer's online activities *over time*—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to deliver advertising targeted to the individual consumer's interests").
[7] Proposed COPPA Rule at 59812.
[8] *See id.* at 59811-59812.

In fact, even if collection for the basic ad metrics described above did not take place the mere use of a third party ad platform by a web publisher would be restricted under the language proposed. For example, if both a kids site and the Wall Street Journal sell their own ads, they both may separately contract to use a service such as DoubleClick's DART for Publishers ad delivery management platform. Each site will upload the ads it has sold and will have separate contracts with DoubleClick calling for confidentiality. The DART system will deliver the ad per the instructions of each publisher. But since DoubleClick uses the same third party cookie for ad delivery across sites, and since it has delivered an ad to a child on one site, under the proposed Rule, it would be deemed to have collected Personal Information about a child when it delivers ads on the Wall Street Journal. This is the case even though it has no legal right to use information from the kids site beyond that site.

Operators also rely on third-party analytics providers. Analytics services reveal how individuals interact with an online service. Although information is collected on a unique user basis, the summary reports are often processed in aggregate form. Analytics providers tell operators how users tend to use a specific app or online service, which functions of a given service are most popular, or how users are able to successful use various services.

Under the proposed Rule, however, third-party analytics providers will be reluctant to contract with operators who provide services to children. To generate a useful analytics report, analytics providers must use persistent identifiers that track users across different online services. Although quality analytics is essential for operators to provide children's online services, it is arguably not necessary for the technical functioning of the Web site or online service, does not satisfy the request of a user, and does not contribute to the security or integrity of the Web site or online service. Under the proposed Rule, therefore, analytics providers who service a children's Web sites or online services and who collect children's personal information would be subject to the proposed Rule's notice and consent requirements.[9]

Those who doubt that being subject to the COPPA Rule would dissuade analytics providers from servicing children's Web sites or online services should take note of Flurry's recent decision to not service children's apps. Flurry, the leading analytics platform for mobile apps, announced on October 25, 2011 that its "[c]ustomers may not use the Flurry Services in connection with any application labeled or described as a 'Kids' or 'Children' application and may not use the Flurry Services a) in connection with any application, advertisement or service directed towards children or b) to collect any personal information of children."[10] This change came soon after the FTC published its proposed modifications to the Rule, because Flurry was worried about being subject to COPPA regulations.[11]

Similarly, a number of operators include social plug-ins on their Web sites to enable users to share news articles and other content across services. These tools result in the operator of the plug-in collecting an IP address or other identifier.

Children's Web sites and apps provide valuable educational and entertainment resources,[12] and those resources are at risk of being impaired by the proposed regulations that would impede advertising and analytics. The FTC therefore should consider modifying the proposed Rule to make sure that third-party analytics providers, social media plug-ins ad networks can provide services to providers of children's online services without being subject to COPPA regulations. FPF suggests that this would best be done through a definition that deems information to be personal when a company tracks children's online activities over time across multiple Web sites and uses that information to create a behavioral profile for the purposes of targeting children with advertising suited to their interests without parental consent.

---

[9] *See id.* at 59812.
[10] Flurry Privacy Policy, Flurry (Oct. 25, 2011), http://www.flurry.com/about-us/legal/privacy.html.
[11] *See* Morgan Reed, *No Analytics for You: How Children's Education Apps Could Suffer Under New Regulations*, Huffington Post (Nov. 7, 2011), http://www.huffingtonpost.com/morgan-reed/app-analytics_b_1072303.html.
[12] *See id.*

The FTC therefore should modify the proposed Rule by defining more narrowly the information as personal when it is collected and used for targeting behavioral advertising, which would then be subject to parental consent.

II. Confidentiality, security, and integrity of personal information collected from children.

Under the proposed Rule, an operator "must take reasonable measures to ensure that any third party to whom it releases children's personal information has in place reasonable procedures to protect the confidentiality, security, and integrity of such personal information."[13] The FTC is right to demand that operators take reasonable steps to ensure that the vendors with whom they contract provide adequate protections for children's personal information. But reach of this regulation goes too far.

FPF suggests that if a third party processes information on behalf of an operator and fails adequately to protect children's information, it is reasonable to impose liability on the operator even if the operator took reasonable steps to ensure that the vendor had adequate protections in place. This conforms with normal business practices, and it would not impose extraordinary duties upon operators. The third party is performing a service that is part of the operator's business, and operators can and should oversee the services performed on their behalf.

But it would not be reasonable to impose liability on operators for *all* third-party failures to adequately protect children's information. Suppose an operator releases children's information to a third party after reasonably ensuring that the third party has adequate protections in place to protect children's information and obtaining parental consent. If the third party processes this information for its own purposes and does not share the fruits of the processing with the operator, the operator should not be liable if the third party fails to reasonably and adequately protect the information. The information processing is not part of the operator's business, and the operator would have little, if any, access to the third party's operations. By taking reasonable measures to ensure that the third party had adequate protections in place, the operator has done all it could do.

Imposing liability on operators for all third-party failures to reasonably and adequately protect children's information would either motivate operators to take *unreasonable* measures to ensure third-party protections or make operators reluctant to deal with third parties in the first place. Either result would have a significant, negative impact on the marketplace for online children's services.

III. Geolocation.

The proposed Rule would consider "[g]eolocation information sufficient to identify street name and name of a city or town" to be personal information.[14] FPF understands that geolocation information has certain characteristics that warrant treating it as "personal information" in certain circumstances.[15] But the FTC should recognize that the nature of geolocation information also warrants that it be appropriately clarified and treated differently than other types of personal information with regard to ongoing data collection.

Operators can collect and store geo-location to identify or contact specific individuals, and this does raise significant privacy concerns. If operators wish to use children's geolocation information in this way, the information is personal and operators should only collect it after obtaining prior parental consent. But operators can also use geolocation information in far less-privacy-sensitive ways—to help children determine where they are or how to find nearby resources. Operators might collect a child's geolocation information in response to the child's request for directions, send directions to the child's device, delete the geo-location information from their records, and never use the geo-location information for any other purpose. Such a uses are valuable for children and should be maintained.

---

[13] *Id.* at 59821.
[14] *Id.* at 59830.
[15] Proposed COPPA Rule at 59813.

Accordingly, the Commission should clarify that geolocation information will only be deemed personal information if it is combined with some other information or identifier, such that it would be possible to contact an individual. This would maintain consistency with the existing Rule.

In fact, under the Rule, operators do not need prior parental consent to collect a child's online contact information to respond to a request from the child provided that the "information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request."[16]

But an important characteristic of geolocation information is that it often supports features that extend over a period of time. Operators cannot provide effective directions if they collect geolocation information only once. A one-time collection of geolocation information does not allow operators to update directions and correct for any wrong turns. The proposed Rule should make clear that under the conditions discussed above, when children request operators to collect their geolocation information to provide a specific service, operators may collect geolocation information continuously or periodically, provided that operators use the geolocation information only for the requested functionality.

For the same reasons discussed in the previous paragraph, the Rule should also make clear that when operators obtain prior parental consent to collect geolocation information for a specified use, the operators may collect geolocation information continuously or periodically, provided the information is used only for the requested functionality. If a particular service is intended to provide a location based service, COPPA should not require a child to make repeated requests simply to continue providing a requested ongoing service.

IV. Apps and Platforms.

An expanded and unnecessarily broad definition of personal information will impose new obligations on many app developers that consider themselves exempt from obligations under COPPA because they are not collecting personal information from kids. A significant number of these developers are individuals including hobbyists, part-timers and teens. They would be hard-pressed to implement parental verification measures.[17] Thus, the changes threaten to impair the rapid growth of the app development sector of the economy.

When a user downloads or enables an app, the platform provides the user's IP address, device ID, username, and account ID to the app developer to enable the app. Under the proposed rule, an app developer is likely to be covered if his app is aimed at children and uses such an identifier. An app may be simply a few lines of code and dependent on the platform for much of its functionality. If the app will only use the personal information provided by the platform for internal operations (including fraud, first party ads, maintaining user settings etc) the Commission should allow app developers to rely on platform providers to provide notice and obtain parental consent on their behalf.

In such a case, the platform provider would provide the parental notification in the online privacy notice and would explain to parents that their children may access and use third-party applications through the platform and that these applications may collect, use, and disclose the child's personal information for the sole purpose of supporting the internal operations of the application.

The platform should provide parents direct notice through a mechanism that allows the parent to identify all of the third-parties that are collecting personal information from their child through the platform at any given time.

---

[16] *Id.* at 59831 (modifying the exception currently in 16 C.F.R. § 312.5(c)(2)).

[17] FPF maintains ApplicationPrivacy.org, a site aimed at providing app developers with privacy resources, including information about COPPA compliance and this is experienced with the compliance issues app developers face.

If an app developer makes information public or enables it to be shared or used more broadly than the limited internal purposes, the app should have to obtain parental consent itself.

The reverse is also true. While an app developer should have flexibility to work with the platform provider, it is the first party app that has primary responsibility for COPPA compliance, including parental notification and consent. The Commission should make clear that an underlying platform or service provider will not be held responsible by virtue of enabling a service or application that is subject to COPPA requirements.

V. New parental consent mechanisms.

The proposed review process should be helpful in advancing innovative ways to obtain parental consent. However, a sixth-month review for products that are ready to be launched is not at all practical in this area of rapid development. We urge a more rapid process when a company can meet certain baseline requirements including providing an effective notice in a manner that parents are likely to receive it and where the method relies on its own records or third party records to support the expectation that the person contacted and responding is the parent. For example, social networks or other companies that have user provided information detailing information and relationships between users can provide a high degree of certainty that an individual is a parent of a specific child. These methods can be more reliable than Commission approved methods such as mailing or faxing consent notices. Companies implementing consent processes that exceed the statutory obligations should be able to receive a rapid Commission review that does not require a more lengthy notice and comment review process.

In general, we believe that additional methods that would allow parents to provide consent for the services they wish to permit their children to use are feasible, but have not been achieved due to numerous factors. We believe the Commission could play an invaluable convening role in encouraging industry to innovate this area. Although COPPA has played a critical role in protecting children's privacy over the last decade, recent evidence about parents helping children lie to gain access to social networking sites makes it clear that the needs of parents and children are not being fully met.[18] Ideas such as enabling verification based on user generated content and confirmed relationships, or platforms helping manage consent for apps or other services, or collaborative privacy portals hold great promise. We urge the Commission to exercise leadership on this aspect of the proposed Rule by convening stakeholders and encouraging the development of consent processes that protect and empower children.

Sincerely yours,

Jules Polonetsky

Christopher Wolf

[18] danah boyd, Eszter Hargittai, Jason Schultz, and John Palfrey. (2011). **"**Why Parents Help Their Children Lie to Facebook: Unintended Consequences of the 'Children's Online Privacy Protection Act**."** *First Monday* 16(11), November, http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075