Before the
FEDERAL TRADE COMMISSION
Washington, DC 20580

COMMENTS

of the

FUTURE OF PRIVACY FORUM

on the

CHILDREN'S ONLINE PRIVACY PROTECTION RULE
Supplemental Notice of Proposed Rulemaking

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

September 24, 2012

Jules Polonetsky
Co-Chair and Director,
Future of Privacy Forum

Christopher Wolf
Co-Chair and Founder,
Future of Privacy Forum
Partner,
Hogan Lovells US LLP

Counsel for the Future of Privacy Forum

I. Introduction

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" or "Commission") for providing this opportunity to comment on the Commission's supplemental proposal to amend the Children's Online Privacy Protection Rule (the "Rule" or "COPPA Rule").[1] 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.[2]

FPF previously filed comments on the Commission's Notice of Proposed Rulemaking published on September 27, 2011 (the "2011 NPRM"), which focused on the proposal's definition of "personal information," the proposed revisions directed to protecting the security, confidentiality and integrity of information collected from children, geo-location issues, apps and platform issues; and the new parental consent mechanisms.

FPF's comments in this filing focus on the proposals contained in the Commission's Supplemental Notice of Proposed Rulemaking ("SNPRM") published on August 6, 2012. In this submission, we address (I) platforms, apps and our proposed amendment to Section 312.4 of the COPPA rule; (II) third party advertising networks and the "internal operations" exceptions; (III); plug-ins; (IV) expansion of the definition of "sites directed to children" and (V) geolocation.

II. Platforms and Apps

One of the newest and most important means by which children access games and educational opportunities today is through the use of Web and mobile applications. From recreation to education, apps have become a central component of a child's online experience. As the app market continues to grow, the Commission is right to be concerned that many of the apps targeting children fail to comply with the FTC's recommended notice and consent mechanisms.[3]

FPF is committed to helping app developers comply with COPPA. We provide a rich online resource for app developers through our Application Privacy site.[4] Leading platform companies like Facebook, Sprint and AT&T point the app developers they interact with to this resource. We also engage with the app developer community through our outreach efforts: last April we held an App Developer conference in San Jose, California, and last week, we led a Mobile App Ecosystem Webinar Briefing for the stakeholders involved in the NTIA Privacy Multistakeholder process.

It is clear that there are a wide range of developers in the app market of varying size and capabilities. In our experience, many do not have the technical and legal expertise to implement

[1] Federal Trade Commission, Supplemental Notice of Proposed Rulemaking and Request for Comment, Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643 (Aug. 6, 2012) (hereinafter "SNPRM").
[2] The views herein do not necessarily reflect those of the Advisory Board or supporters of the Future of Privacy Forum.
[3] FTC Staff Report: Mobile Apps for Kids: Current Privacy Disclosures Are Dis*app*ointing (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
[4] http://www.ApplicationPrivacy.org

a COPPA compliant age verification solution. One solution for this challenge is to allow apps to satisfy COPPA age verification and other obligations by relying on a common mechanism that would serve many apps. Under the proposed rule, a platform that offers apps to its customers would be highly unlikely to offer such an opportunity to developers because of the broad liability they might shoulder if they were considered an operator of those apps. Although platforms range in the level of review or oversight they provide for the activity of apps, we are certain that no platform could reasonably commit to being responsible under COPPA for the activity of hundreds of thousands of apps.

In addition to the fact that the Commission's proposal to expand COPPA obligations to many new operators would present practical challenges for these entities — the majority of which, the Commission acknowledges, are small businesses that may not already have the resources to do so — we believe that expanding the scope of COPPA obligations could significantly increase the burdens on parents as well. This is because parents will be expected to receive many more notices from operators and give more consents than they are today, in a process that already may be overwhelming for parents of children who use the Internet regularly. Although it is not possible to eliminate these burdens, we agree with the Commission that one way to reduce them is to encourage entities to collaborate by consolidating notices and obtaining centralized consents, where doing so is feasible and clear to parents.

FPF, like several other commenters, encouraged the Commission to take steps to facilitate this kind of collaborative compliance in our 2011 comments, and we continue to believe that a rule change along these lines is important to making it practicable for operators to comply with COPPA and reducing the burdens on parents associated with the COPPA process. In order to provide parents with the ability to approve apps that they want to be available to their children in a manner that provides a reliable consent mechanism and robust parental controls, we propose the following amendment to Section 312.4 of the rule:

Proposed Amendment to Section 312.4 of the COPPA Rule

(b) *Notice on the Web site or online service.* Pursuant to § 312.3(a) *and subject to paragraph (c)*, ~~*each*~~ *an* operator of a Web site or online service directed to children must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, and, at each area of the Web site or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience Web site or online service that has a separate children's area or site must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the Web site or online service's information practices must state the following:

(1) ~~*Each*~~ *The* operator's contact information, which at a minimum, must include the operator's name, physical address, telephone number, and e-mail address;

(2) A description of what information ~~*each*~~ *the* operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how such operator uses such information, and; the operator's disclosure practices for such information; and,

(3) That the parent can review and have the child's personal information deleted, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

(*c) Common mechanism. Multiple operators that provide content or services using a common platform (including a Web site, network, or collection of services) may provide notice, obtain verifiable parental consent, or comply with other obligations under this Part through a common mechanism that satisfies the requirements described in this subsection.*

(1) Notice. An operator that chooses to satisfy its notice obligations through a common mechanism shall ensure that, before obtaining verifiable parental consent, the common mechanism provides one of the following or a link thereto:

(A) a means by which the parent can access the names of each operator that relies on the common mechanism and the online notice describing how each operator collects, uses, and discloses personal information collected from children under 13 (which may include individual notices for each operator or, if the operators all conform to a common practice, a consolidated notice); or

(B) a general notice that states the following:

(i) that multiple operators may provide Web sites or online services as a part of the platform;

(ii) a description of the types of Web sites or online services that the operators provide;

(iii) that the operators may collect and maintain personal information collected from children under 13;

(iv) a list of the specific items of personal information that each operator may access or collect from such children through the platform, where such access or collection must be reasonably related to the functionality that the operator offers to users of its Web site or online service; and

(v) a general description of the manner in which participating operators may collect, use, and disclose the personal information from such children through the platform.

(2) Parental control. When a child uses or installs for the first time a Web site or online service that is made available through the common mechanism, the operator shall ensure that the parent is provided with a means by which the parent can:

(A) access the name of the operator and online notice of its information practices with regard to children or a link thereto, and

(B) prevent the child's future use of the Web site or online service through the common mechanism, including through revocation of the consent that the parent provided through the common mechanism.

(3) Limits on further information collection and use.

(A) Generally. An operator that chooses to satisfy its consent obligations through a common mechanism shall ensure that its notice discloses a means by which the parent can delete the personal information that the operator accessed through the common mechanism.

(B) Preapproval of additional personal information collection. If an operator using the common mechanism to obtain verifiable parental consent wishes to receive items of personal information from a child other than those disclosed in the notice described in subsection (c)(1), the operator shall obtain verifiable parental consent in advance of the collection, use, and disclosure of such information, and may do so through the common mechanism.

(C) Preapproval of additional uses or disclosures. If an operator using the common mechanism to obtain verifiable parental consent wishes to use personal information that it collected from a child through the common mechanism for a purpose other than that disclosed by the common mechanism as described in subsection (c)(1), the operator may use the common mechanism to enable parents to provide specific advance consent to the additional use or disclosure of personal information.

(4) Other obligations. An operator may choose to satisfy one or more of its other obligations under this Part through the use of a common mechanism. In such event, the use of the common mechanism shall not modify the general requirements applicable to the operator's obligation, except as expressly set forth in this subsection.

(5) Liability of operators and common mechanism providers.

(A) Liability of operators. An operator's participation in or provision of a common mechanism shall not limit its liability under this Part. However, no operator shall be liable for violations of this Part by another operator solely on the basis that both operators participate in a common mechanism.

(B) Liability of common mechanism providers. A provider of a common mechanism shall not be deemed an operator of another operator's Website or online service for the purpose of this Part by virtue of its provision of the common mechanism, nor shall it be liable for violations of this Part by operators that participate in its common mechanism. However, the provider shall retain its obligations under this Part for any Web site or online service of which it is the operator and may be liable for its independent violations of 15 U.S.C. 57a that do not arise out of violations committed by an operator participating in the common mechanism.

(C) Number of violations. A violation of this Part or of 15 U.S.C. 57a that is associated with a common mechanism shall be deemed a single violation even if the violation affects multiple operators, Web sites, or online services.

(6) Data minimization. To the extent that the provider of a common mechanism is an operator of a Web site or online service, its compliance with this subsection shall not relieve it of its obligation to comply with section 312.3(d) with respect to its Web site or online service.

We propose the above requirements for platforms that seek to take on the additional responsibility of providing a common consent mechanism. For those that do not, the operators participating in the platform could continue to satisfy their own COPPA obligations as they do today. In either case, we think the FTC should clarify that platforms should not be responsible under COPPA for the data collection activity of third parties using their platform.

III. Third Party Advertising Networks and "Internal Operations" Exception

In our previous comments, we endorsed the Commission's efforts to ensure that children are not the subjects of online behavioral advertising.[5] FPF appreciates the Commission's focus on ensuring that children are not "behaviorally targeted."[6] We agree that the current rule and current industry standards leave a gap that needs to be closed. Under the current rule or current standards, a child directed site could directly contract with an ad network for behavioral

[5] *See* Future of Privacy Forum (comment 55) at 2-4.

[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").

advertising. The current rule would not restrict this activity, although current industry standards do restrict behavioral ads specifically targeted to be children. We appreciate the intention of the Commission to close this gap.

However, our previous comments flagged concerns related to the way the proposed definition of "personal information" would affect the logging of unique identifiers that function across multiple websites for activities that are *unrelated* to behavior advertising, including basic ad delivery and reporting.

The FTC's new proposed changes partially address this concern by seeking to exempt parties from COPPA obligations when personal data is being used for internal operations, including personalization and contextual advertising.[7] We are uncertain whether this language clearly exempts the range of legitimate uses that a third party service may need when logging a unique identifier across sites.

Thus, we propose the FTC clarify that "internal operations" covers analytics, advertising and related reporting.

The proposed rule further intends to modify the definition of a website or online service directed to children to include any operator who "knows or has reason to know" it is collecting personal information through a host website or service directed to children.[8] The FTC notes that third parties like ad networks do not have a duty to "monitor or investigate whether their services are incorporated into child directed properties."[9] However, the FTC makes clear that "such sites and services will not be free to ignore credible information brought to their attention indicating that such is the case." The FTC seeks to avoid covering all third parties, simply because they provide code that can be downloaded by any web site. However, we believe that this standard continues to leave a wide range of third parties who have no way of knowing how their services are used subject to the rule.

The FTC should clarify that a third party that collects identifiers across sites has "actual knowledge" only in a more clearly defined set of circumstances. For example, the following cases should be considered covered by the definition:

1. The third party targets children under 13 for advertising based on activity on unrelated web sites.

2. The web site has expressly contracted or provided instructions to the third party requiring that ads or content inappropriate for children under 13 be restricted from the site.

IV. Plug-Ins

[7] SNPRM at 46647.
[8] SNPRM at 46645.
[9] SNPRM at 46643.

Notwithstanding the above discussion, we think certain types of plug-ins that do expressly collect personal information on child directed sites should be treated differently and excluded from the definition of "actual knowledge or reason to know." If a plug-in simply collects explicit personal information on a child directed site, certainly the operator of that plug-in should be subject to the same obligations posed on the site. But when the provider of a plug-in has elsewhere provided an age screening mechanism, and a child directed site provides that plug-in on its pages so that parents or teens can make use of that plug-in, it should not be covered. Here the operator of the plug-in has explicit reason to know that the web site visitors it interacts with are not under 13!

V. Expansion of the Definition of Sites Directed to Children

We are concerned about the FTC's proposal to amend the definition of "directed to children" to specifically address sites "likely to attract an audience that includes a disproportionately large percentage of children." This change could be read to mean that teen sites, Wikipedia, and many general audience sites will for the first time be captured by the scope of COPPA, creating potential age screening or verification obligations that would burden access to content for an adult audience. We believe this is an unreasonable imposition on the general web audience and poses constitutional concerns. The Commission should clarify that subsection (c) is intended to be a subset of sites that are directed to children under the Commission's longstanding totality of the circumstances test based on the factors in the definition.

VI. Geolocation.

We are aware that the SNPRM does not directly address location, but we are concerned that the substantial changes proposed in the NPRM regarding location are further emphasized by the SNPRM. As such, we reiterate here the concerns we raised in our previous filing.
The proposed Rule would consider "[g]eolocation information sufficient to identify street name and name of a city or town" to be personal information.[10] FPF understands that geolocation information has certain characteristics that do warrant treating it as "personal information" under certain circumstances.[11] However, 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 geolocation to identify or contact specific individuals; 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. Yet operators can also use geolocation information in far less-privacy-sensitive ways: i.e. 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 geolocation information from their records, and

[10] Federal Trade Commission, Notice of Proposed Rulemaking and Request for Comment, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, 59830 (Sept. 15, 2011) (hereinafter "NPRM").
[11] NPRM at 59813.

never use the geolocation information for any other purpose. Such a uses are valuable for children and should be maintained.

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."[12]

However, 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.

We thank you for the opportunity to provide these comments and look forward to working with the Federal Trade Commission.

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