MEMORANDUM

TO: ESPC

FROM: D. Reed Freeman, Jr.

DATE: January 3, 2013 FILE: 68223-0000001

RE: Revised COPPA Rule

We write this memo to update you regarding the Federal Trade Commission's ("Commission") recently announced revisions to its rule implementing the Children's Online Privacy Protection Act ("Rule").[1] The changes – which take effect on July 1, 2013 – are significant. They alter the scope and obligations of the Rule in a number of ways. We discuss the revisions, which include the following, in greater detail below:

- ***The Commission revised the Rule's definition of "personal information" to include more types of data that trigger the Rule's notice, consent, and other obligations. These include persistent identifiers when used for online behavioral advertising and other purposes not necessary to support the internal operations of the site or online service.***

- ***The Commission expanded the Rule's coverage to third-party services – such as ad networks and social plug-ins – that collect personal information through a site or service that is subject to COPPA. The host site or service is strictly liable for the third party's compliance, while the third party must comply only if it has actual knowledge that it is collecting personal information through a child-directed site or from a child.***

- ***The Commission streamlined the content of the parental notice and simplified the privacy policy.***

- ***The Commission retained the "email plus" method of obtaining parental consent. It also added new methods of obtaining consent and established a process for pre-clearance of other consent mechanisms.***

- ***The Commission imposed new data security pass-through requirements, as well as data retention obligations.***

---

[1] The Commission's press release announcing the final revised Rule is available at http://www.ftc.gov/opa/2012/12/coppa.shtm.

- ***The Commission revised the Rule to permit certain sites that are "directed to children" to comply only with respect to those users who self-identify as under 13.***

* * *

1. <u>The Commission revised the Rule's definition of "personal information" to include more types of data that trigger the Rule's obligations.</u>

Under the Rule, the online collection of "personal information" from a child generally triggers an operator's obligation to provide notice to a parent, obtain the parent's verifiable consent, and comply with other requirements. The Commission has expanded the definition of "personal information" to include the following new elements:

- ***A photo, video, or audio file*** that contains "a child's image or voice." Currently, the Rule deems a photo to be personal information only if it is combined with other information that permits the contacting of a child. The Commission justified doing away with that condition with the reasoning that photos, videos, and audio files are inherently personal and may, on their own, be used to identify individuals if, for instance, they are embedded with geolocation data, paired with physical location data, or analyzed with facial recognition software.

- ***Geolocation information***, if it provides information at least equivalent to street name plus city or town. It does not have to be as precise as street number.

- ***Online contact information***, which is currently defined as "an e-mail address or any other substantially similar identifier that permits direct contact with a person online." The revised Rule adds the following illustrative examples: an instant messaging user identifier, a Voice over Internet Protocol identifier, and a video chat user identifier.

- ***Screen or user name***, when it functions as "online contact information," as defined above.[2] In its statement of basis and purpose for the revised Rule, the Commission addressed the concern that the inclusion of screen and user names in the definition of "personal information" would limit operators' ability to offer interactive features because they would be constrained by the attendant compliance obligations. The Commission explained that the definition is intended to cover "direct, private, user-to-user contact" and not the use of anonymous screen or user names for purposes of content personalization, filtered chat, public display, operator-to-user communication, or to allow children to log in across devices or related properties. Accordingly, the revision should generally not affect operators' ability to use user or screen names in place of individually identifiable information and thereby avoid triggering the Rule's obligations.

[2] Under the current Rule, a screen or user name does not fall within the definition of "personal information" unless it contains an individual's email address.

- ***A persistent identifier***, such as a customer number held in a cookie, an IP address, a processor or device serial number, or a unique device identifier,[3] where it can be used to recognize a user over time and across different sites or online services[4] – but only when used for functions other than or in addition to support for the internal operations of the site or service. This means that:

    - *An operator does not have to comply with the Rule's notice, consent, and other obligations if it uses persistent identifiers solely to support its internal operations.*[5] The Rule defines such "support" as only those activities necessary to do any of the following, provided that the information collected is not used or disclosed to contact a specific individual (including through behavioral advertising), to amass a profile on a specific individual, or for any other purpose: (1) maintain or analyze the functioning of the site or service; (2) perform network communications; (3) authenticate users of the site or service; (4) personalize the content on the site or service;[6] (5) serve contextual advertising on the site or service;[7] (6) cap the frequency of advertising; (7) protect the security or integrity of the user, site, or service; (8) ensure legal or regulatory compliance; or (9) fulfill a permitted request of a child.[8] The revised Rule permits a party to seek approval of additional activities to be included within the "internal support" definition. The Commission will publish and seek comment on such a request and respond to it within 120 days.

    - *An operator must comply with the Rule's notice, consent, and other requirements if it uses persistent identifiers for any other purpose, including retargeting and other behavioral advertising.* According to the Commission, the activities enumerated within the "internal support" definition are intended to be narrowly construed. If a persistent identifier is used for any non-enumerated purpose, it is "personal information" and triggers the Rule's requirements. As a practical matter, it may be difficult to comply in certain circumstances. For example, it is not clear how a site not directed to children

[3] The Rule currently provides that persistent identifiers constitute "personal information" – and thus trigger the Rule's obligations – only when they are associated with individually identifiable information, such as name, address, email address, phone number, or Social Security number.

[4] The term "different" means either sites or services that are unrelated to each other or sites or services where the affiliate relationship is not clear to the user.

[5] The Rule also provides an exception for persistent identifiers collected through affirmative interaction by users who have previously been age-screened and are not children.

[6] According to the Commission, "personalizing content" would permit operators to, for example, maintain user-driven preferences, such as game scores or character choices in a virtual world.

[7] Contextual advertising is "the delivery of advertisements based upon a consumer's current visit to a web page or a single search query, without the collection and retention of data about the consumer's online activities over time." *See* Preliminary FTC Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," (Dec. 2010), at 55 n. 134, *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf.

[8] The Commission's statement of basis and purpose for the revised Rule notes that the following activities are included within the definition's categories: intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, and de-bugging.

but still subject to the Rule (because it knowingly collects personal information from children) will identify which of its users are children and for whom parental consent is required before it may drop a persistent identifier for retargeting purposes.

During the long rulemaking proceedings, industry strenuously objected to the Commission's proposal to include persistent identifiers within the definition of "personal information," arguing that such information is associated with a device and not an individual. The Commission ultimately disagreed, determining that persistent identifiers fall within the definition because they permit the online contacting of a specific individual. This should not come as a surprise, as the Commission has repeatedly stated in recent years that the line between what has traditionally been considered "personal" and "non-personal" information is increasingly blurred, such that the protections historically afforded to personal information should be extended to certain non-personal information as well. With the codification of the Commission's position in the revised Rule, industry is on notice that the Commission will likely continue to take the same approach in other contexts.

2. <u>The revised Rule covers third-party services that collect personal information through a child-directed site or service: the host site or service is strictly liable for the third party's compliance, while the third party must comply with the Rule only if it has actual knowledge that it is collecting information through a child-directed site.</u>

The Commission has set forth new standards for which party (or parties) is liable for COPPA compliance when a third-party service – such as an ad network or a social plug-in – is integrated into a child-directed site or service. Specifically:

- ***The host operator is responsible for the activities of a third party that collects personal information on the host's site or service if: (1) the third party is an agent or service provider of the host or (2) the host benefits by allowing the third party to collect personal information directly from users.***[9] This revision reflects a shift from prior Commission statements indicating that an entity had to have ownership, control, or access to the personal information at issue in order to be liable as an operator. The Commission has now taken the position that a strict liability standard is appropriate because the host is in the best position to know and control which plug-ins, software downloads, and other services it integrates into its site and is also in the best position to give notice and obtain consent from parents. The change will require an operator to carefully review whether the data collection activities of any service it permits to operate on or through its site or service subject it to the Rule and, if so, to carefully vet and monitor the third party's compliance (or to assume compliance responsibility for it).

[9] The "benefit" to the host site or service could be, for example, through the addition of content, functionality, or advertising revenue. The Commission explains in its statement of basis and purpose that platforms – such as those that offer mobile apps – are not liable if they merely offer access to content provided by others.

Importantly, the Commission notes (though only in a footnote in its statement of basis and purpose) that, "[a]lthough this issue is framed in terms of child-directed content providers integrating plug-ins or other online services into their sites because that is by far the most likely scenario, the same strict liability standard would apply to a general audience content provider that allows a plug-in to collect personal information from a specific user when the provider has actual knowledge the user is a child."

- ***A third party that collects personal information through another operator's site or service – such as an ad network or a social plug-in – will be considered "directed to children" and therefore itself subject to the Rule if it has actual knowledge that it is collecting personal information from users of a site or service directed to children.*** The Commission declined to impose a strict liability standard on such third parties, recognizing the logistical difficulties that they face in controlling and monitoring the sites that incorporate their services. That said, the Commission's statement of basis and purpose for the revised Rule suggests that the "actual knowledge" standard may not be difficult to meet. Specifically, the Commission explains that the standard will generally be met when: (1) the host site or service communicates to the third-party service about its child-directed nature, or (2) a representative of the third-party service recognizes the child-directed nature of the host's content.[10] This test could raise compliance issues, since whether or not a particular site or service is "directed to children" under the Rule is a question that involves multiple factors and may not be readily ascertainable by employees of the service. Moreover, given that the service could be held liable for the knowledge of any one of its employees, it must train them to take appropriate action in the event that they believe that the host site or service could be child-directed.

3. <u>The revised Rule streamlines the parental notice requirements.</u>

An operator subject to the Rule must provide parents with notice of its information practices in two ways: in a notice delivered directly to the parent and on the site or service itself (typically through the posting of a privacy policy). The Commission has revised the Rule to rely less on the posted privacy policy and more on the direct notice because it believes that the direct notice gives a parent the best opportunity, at the most appropriate point in time, to evaluate the operator's information practices and determine whether to permit his or her child to share personal information with it. Specifically:

- ***Direct notice to parents:*** Under the revised Rule, the direct notice is intended to work as an effective "just-in-time" communication to a parent about the operator's information practices. This approach is consistent with the Commission's view that the most effective privacy notices are clear and concise and offered in a context in which an individual is making a privacy-related decision.[11] Accordingly, the

[10] The Commission explains that these two examples are not exhaustive, and "an accumulation of other facts" could also establish actual knowledge.

[11] *See* "FTC Releases Draft Privacy Report Outlining Best Practices, Possible New Requirements Under Section 5 of the FTC Act, and Expressing Support for a 'Do Not Track' List" (Dec. 3, 2010), at

Commission has revised the Rule to prescribe the disclosures that must be made in each type of direct notice,[12] to ensure that a parent receives key information up front and is directed, via link, to the full privacy policy for additional information.

- ***Online notice (the privacy policy):*** The revised Rule streamlines the content of the COPPA privacy policy by requiring that it include only: (1) the operator's contact information;[13] (2) the information that the operator collects from children, including whether the site or service permits a child to make personal information publicly available, such as through a message board or chat room; (3) how the operator uses such information; and (4) its disclosure practices. The revised Rule also includes streamlined requirements for placement of the privacy policy on the site or service. Substantively, the requirements are consistent with the current Rule. With respect to mobile apps, the Commission's statement of basis and purpose explains that the online notice must be placed on the app's home or landing screen; it does not require that the notice appear at the point of purchase, though the Commission encourages that as a best practice.

4. <u>The revised Rule retains the "email plus" method of obtaining parental consent, adds new methods of obtaining consent, and sets out a process for pre-clearance of other consent mechanisms.</u>

- ***The Rule retains the "email plus" method of obtaining parental consent and establishes a pre-approval process for new methods.*** The Rule sets forth a two-tiered system for obtaining parental consent: an operator that uses a child's personal information only internally may continue to use the so-called "email plus" consent mechanism (which involves an email from the parent coupled with an additional step), while more foolproof measures are required if the operator will disclose the child's personal information to a third party. During its review of the Rule, the Commission considered eliminating this distinction, on the grounds that "all collections of children's information merit strong verifiable parental consent." Persuaded by the weight of comments that, although imperfect, email plus remains a valued and cost-effective consent mechanism for certain operators, the Commission decided against this. This is significant because "email plus" is the most common way of obtaining consent. The Commission does not, however, give it a ringing

---

http://www.mofo.com/files/Uploads/Images/101203-Do-not-track-list.pdf.

[12] The type of notice depends on the type of consent sought: Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information; Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times (such as via a newsletter); Notice to a Parent in Order to Protect a Child's Safety; and Voluntary Notice to a Parent of a Child's Online Activities Not Involving the Collection, Use, or Disclosure of Personal Information. The last type of notice is new. It corresponds to a new exception to parental consent which gives an operator the option to collect a parent's online contact information for the purpose of providing notice of a child's participation in a site or service that does not otherwise collect, use, or disclose children's personal information. The parent's online contact information may not be used for any other purpose, disclosed, or combined with any other information collected from the child.

[13] As under the current Rule, the revised Rule requires that all operators be listed in the privacy policy but permits multiple operators to designate just one as the point of contact. During its rule review, the Commission had considered requiring disclosure of all operators' contact information but decided against doing so.

endorsement and urges the creation of new methods of consent. To that end, the revised Rule sets forth a voluntary approval process for new methods of obtaining verifiable parental consent.[14]

- ***The revised Rule adds methods for obtaining parental consent.*** The Commission has made clear that the Rule's list of methods of obtaining consent is non-exhaustive. With the revised Rule, the list now includes: (1) electronic scans of signed consent forms; (2) videoconferencing; (3) collection of a parent's government-issued identification and checking it against a database (provided that the operator takes certain steps to protect the parent's privacy); and (4) the use of an online payment system, as long as the system provides notice of each transaction to the primary accountholder.

5. <u>The revised Rule imposes new data security and data retention obligations.</u>

- ***The revised Rule imposes pass-through data security obligations.*** The existing Rule requires an operator to maintain procedures to protect the confidentiality, security, and integrity of children's personal information. The revised Rule strengthens that obligation by requiring an operator to take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining its confidentiality, security, and integrity and who provide assurances that they will do so. This obligation covers only business-to-business disclosures and not, for example, the disclosure of a child's personal information through a site's social networking-type feature. Moreover, the obligation does not require an operator to "ensure" that third parties secure the released information absolutely – a standard the Commission had originally proposed. Instead, an operator "must inquire about entities' data security capabilities and, either by contract or otherwise, receive assurances from such entities about how they will treat the personal information they receive."

- ***The revised Rule imposes limits on data retention.*** Because the Commission views the deletion of unneeded personal information as an integral component of a reasonable data security program, it has added a new section to the Rule that requires an operator to retain personal information "for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." Thereafter, the information must be deleted in a manner that safeguards against a breach.

6. <u>The revised Rule makes a few additional noteworthy changes.</u>

- ***The revised Rule adds factors for determining whether a site is "directed to children."*** The revised Rule retains its multi-factor analysis for determining whether a site or service is "directed to children," with the addition of musical content and the

[14] Under this process, an applicant will submit a description of the proposed consent mechanism. The description will be published in the Federal Register for public comment and then approved or denied by the Commission within 120 days.

presence of child celebrities or celebrities who appeal to children as factors in the analysis.

- ***The revised Rule permits certain sites that are "directed to children" to comply only with respect to those users who self-identify as under 13.*** A site or service that fits within the Rule's definition of "directed to children" but that does not target children under 13 as its primary audience can be deemed not "directed to children" if it age screens all users and then provides notice and obtains parental consent (and otherwise complies with the Rule) only with respect to those who indicate that they are under 13.

  On the other hand, a site or service that targets a primary audience of children under 13 must continue to presume that all users are children, subject to the requirements of the Rule. The Commission provides little guidance on what it means to target a "primary audience" of children. In its statement of basis and purpose, it explains that the determination must be based on the totality of the circumstances and not on some precise threshold cut-off.

- ***The Commission has clarified that the "collection" of personal information includes the provision of open data fields.*** The Rule's definition of "collects" and "collection" still means "gathering of any personal information from a child by any means," but the Commission has expanded the non-exhaustive description of what such gathering entails to include "prompting" or "encouraging" a child to submit personal information online. The change clarifies the Commission's longstanding position that "an operator that provides a field or open forum for a child to enter personal information" is subject to the Rule, even if the submission of personal information is not mandatory.

- ***The Commission has replaced its 100% deletion standard for publicly posted information with a standard based on reasonableness.*** The current Rule's definition of "collection" includes "enabling children to make personal information publicly available . . . except where the operator deletes all individually identifiable information" from postings before they are made public, as well as from the operator's own records. Having determined that this "100% deletion standard" is unrealistic, the Commission has replaced it with a "reasonable measures" standard. Accordingly, no "collection" of personal information takes place – and the Rule is therefore not triggered – if an operator takes "reasonable measures to delete all or virtually all personal information" before a posting is made public. This revision is likely to encourage operators who wish to offer interactive features without triggering the Rule's notice and consent obligations.

* * *

The revised Rule should prompt all sites and online services, and those third parties that collect information from children on such sites and services, to take a fresh look at their practices. Some will be newly subject to the Rule's requirements. Others, already covered

by the Rule, will have to review their compliance procedures to determine whether any changes are needed. At the very least, those already in compliance will have to re-work their parental notices and privacy policies before the revised Rule takes effect on July 1, 2013.