CLIP Center on Law and Information Policy
AT FORDHAM LAW SCHOOL

COPPA Rule Review, 16 C.F.R. Part 312, Project No. P104503

The Center on Law and Information Policy of the Fordham University School of Law ("CLIP") appreciates the opportunity to comment on the proposed amendments to the Children's Online Privacy Protection Rule ("COPPA Rule") as published at 76 Fed. Reg. 59804 (Sept. 27, 2011).

CLIP is an academic research center founded in 2005 to address the emerging field of information law. Among its activities, CLIP seeks to advance solutions to legal and policy problems in the field, including information privacy law and policy, through independent, scholarly research. CLIP has conducted research on children's privacy and has developed expertise in this area through its work on an extensive 2009 report "Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems."[1] CLIP is staffed by an academic director, Professor Joel R. Reidenberg, an executive director, Jamela Debelak, a dean's fellow, Jordan Kovnot, and student research fellows.

Our comments on the proposed amendments to the COPPA Rule suggest multiple ways in which the proposed amendments can be strengthened to further protect parents' right to control information collected from their children. In proposing the current amendments, the FTC has made important progress towards ensuring that the rule applies to new technologies. When it enacted COPPA, Congress authorized the FTC to regulate the collection of information from children when that information "permits the physical or online contacting of a specific individual."[2] COPPA was created to give parents an effective way to limit how personal information about their children is collected and used. We commend the FTC for updating the rule in order to account for advances in mobile technologies and social networking trends.

Respectfully, we offer the following comments and suggestions. Our comments will focus on (1) the classification of screen names; (2) the "de-anonymization" of demographic data; (3) the regulation of behavioral advertising networks in relation to children; (4) consent mechanisms; and, (5) the establishment of clear standards for data deletion.

1. Inclusion of Screen Names as Personal Information in § 312.2

The FTC proposes treating screen names as personal information, even when not paired with other forms of personal information. This is a positive step that reflects the realities

[1] *Available at* http://www.law.fordham.edu/childrensprivacy.

[2] Children's Online Privacy Protection Act, 15 U.S.C.A. § 6501 (8)(f) (1998). *See also* 144 Cong. Rec. S11657 (Oct. 7, 1998) (Statement of Sen. Bryan) describing one of the law's purposes as enhancing "parental involvement to help protect the safety of children in online fora . . . in which children may make public postings of identifying information."

of how children (and Internet users of all ages) are managing their digital identities. However, the commission has also created several "internal use" exceptions that would exempt screen names from COPPA compliance. As discussed below, one of these "internal use" exceptions undermines this important update to the rule.

An increasing number of platforms permit or require the use of screen names as user identifiers. Users commonly maintain one screen name across multiple platforms. Thus, a child might use the same screen name to comment on a blog, play an online video game via Xbox live, video chat over Skype, or instant message with friends. From the perspective of the child user, maintaining a consistent screen name across platforms is a way to build a digital identity. This construction of a digital identity is something of critical importance to children as more and more of their social lives take shape in the digital space. As a result of cross-platform practices, an adult user interacting with a child on one platform would be easily able to identify the same child on a different platform when an identical screen name appears in both places. In this way, the proliferation of screen names, and the likelihood that a child will use a consistent screen name across platforms, enables a specific child to be identified and contacted. As such, it is entirely appropriate for the commission to categorize screen names as personal information.

We are, nevertheless, concerned about one of the newly defined permissible purposes for the use of screen names. The proposal indicates that screen names will not be considered personal information, and will not trigger COPPA compliance, when they are used for "internal purposes." In discussing the permissible internal purposes for screen names, the FTC's proposal lists three possible uses: "for access to the site or service, to identify users to each other, and to recall user settings."[3] In carving out these exceptions, the FTC is cognizant of the fact that these identifiers *can* point to specific users, but that processing them is often essential to the functionality of websites.

We agree with the commission that using screen names in a functional, internal way should not *per se* trigger COPPA compliance. Two of the three suggested permissible purposes- the use of screen names for site access and implementing user settings- are valuable functional uses that are justified as permissible purposes. In both instances, screen names need only be shared between two parties: the user and the site operator. Although COPPA is designed to govern the flow of information that might be used to contact a child user, here that contact is an essential aspect of presenting a site to the user. Importantly, when used in this limited way, no third parties are presented with the child's screen name.

In contrast, the third exempted internal use of screen names, "to identify users to each other," does not function in such a limited way and risks exposing children to the type of contact that parents may not condone. Unlike the other proposed permissible purposes, the disclosure of a child's screen name to other users is not a two-way interaction between the user and the site operator. It is a multi-party interaction which takes a data point that can be used to identify a child and makes it available to multiple other users of a site. This is exactly the type of use that requires parental consent under the COPPA statute itself. As such, using screen names to *identify* users to each other should not be considered an internal use in that *external* parties (other than the user and operator) will be able to view the screen name and use it. We believe this use is precisely the type of use that should require parental consent under COPPA and not be granted an internal use exemption.

[3] Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804, at 59810 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312).

2. Inclusion of ZIP, Date of Birth, Gender and ZIP+4 as Personal Information in § 312.2:

In response to the FTC's questions about the anonymity of combinations of demographic data, we believe that the combination of date of birth, gender and ZIP code should be considered personal information for the purpose of COPPA compliance.[4] Numerous studies have shown that combining these data points is sufficient to identify a specific individual user. For example, scholars have shown that using technology available more than a decade ago, approximately 87% of the U.S. population could be identified using the combination of birthday, gender and ZIP code.[5] Technological advances in the past decade have made it possible to go beyond this and re-identify individuals based on metrics such as browser settings, movie reviews, search terms, and browsing habits.[6] At a minimum, the combination of ZIP code, date of birth, and gender should be categorized as personal information. Other combinations of demographic data might also warrant inclusion within the definition of personal information.

With respect to ZIP+4 data, any combination of ZIP+4 data with another piece of demographic information may be sufficient to identify a user. For example, the likelihood that two residents within the same ZIP+4 zone share the same date of birth or web browser configuration is very low. Because COPPA is designed to give parents control over the disclosure of their children's information and because these data points (date of birth, gender, ZIP and ZIP+4), when combined with other unrestricted data, can so easily be identified to specific children, the commission should include the combination of this data in its definition of personal information.

3. The Regulation of Behavioral Advertising in § 312.2:

The proposed amendments would treat any identifier "that links the activities of a child across different websites or online services" as personal information.[7] The FTC states explicitly that this means parental consent will now be required before persistent identifiers are used for behavioral advertising on children's sites or when an advertiser has actual knowledge that a user is a child. This is a positive step and reflects COPPA's underlying purpose to give parents the decision-making authority over the privacy of their children's information. However, the proposed amendments contain a noteworthy weakness that is not consistent with the goal of protecting children's privacy and parental choice. The amendments do not appear to place limits on those advertising networks that collect data from children on general audience sites when those sites and networks have not collected a child's specific age, but nonetheless have knowledge that a child is under 13. The FTC should make clear that compliance is required in

---

[4] Children's Online Privacy Protection Rule, 76 Fed. Reg. at 59828 (proposed Sept. 27, 2011).

[5] Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population*, (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4, 2000). *See also* Paul Ohm, Public Comment no. 48 on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Act Through the Children's Online Privacy Protection Rule (June 30, 2010) *and* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* 57 UCLA L.Rev. 1701 (2010).

[6] Seth Schoen, *What Information is "Personally Identifiable"?*, Electronic Frontier Foundation. (Sep. 11, 2009, 10:43 PM), https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable.

[7] Children's Online Privacy Protection Rule, 76 Fed. Reg. at 59812 (proposed Sept. 27, 2011).

instances when acquired demographic data, aggregated across multiple sites, is used by a behavioral advertising network to profile a particular user as a child under 13 for the purpose of serving advertisements for that demographic to the user.

The FTC has previously recognized that advertising networks can be regulated under COPPA. In its issuance of the final COPPA rule in 1999, the FTC made clear that the rule applied to advertising networks, including those that place ads on non-children's sites.

> [I]f such companies collect personal information from visitors who click on their ads at general audience sites, and that information reveals that the visitor is a child, then they will be subject to the Act. In addition, if they do not collect information from children directly, but have ownership or control over information collected at a host children's site, they will be considered operators.[8]

In addition, the original 1999 rule explicitly stated that collecting the specific age from a user is not the only way for an operator to acquire actual knowledge for the purpose of triggering compliance. Demographic data about a user can also alert an operator to a user's age. In 1999 the FTC warned operators that it would

> examine closely sites that do not directly ask age or grade, but instead ask ''age identifying'' questions, such as ''what type of school do you go to: (a) elementary; (b) middle; (c) high school; (d) college.'' Through such questions, operators may acquire actual knowledge that they are dealing with children under 13.[9]

For example, while a site capturing data that indicates a user is in middle school would not necessarily provide sufficient information to determine if the user is above or below age 13, data that indicates a user is in elementary school (or college) would provide a much clearer picture. Thus, demographic data can provide actual knowledge that a child is under 13 without ever knowing the child's *specific*, numeric age.

We believe that regulation of behavioral advertising networks is appropriate because they have the ability to collect a staggering quantity of highly personalized data about users. The data collected, even when "anonymized," can often identify *specific* individuals and allow for the development of complex profiles of those users and their habits. Some of this data (such as education levels, areas of interest, activities, type of sites visited and frequency of visits) may not always provide information sufficient to ascertain a specific age, but when an advertising network collects sufficient information to profile a specific user as younger than 13 for purposes of serving advertisements, COPPA protections should apply. While such profiling is conducted in order to deliver relevant advertising content (content whose revenues subsidize much of the beneficial and free content and services available on the web), this justification does not alleviate privacy concerns.

In instances in which aggregated demographic data is processed by an advertising network to profile a user as a child under 13, the FTC should require compliance with the rule. This goes to the heart of COPPA. Behavioral advertising is, by its very nature, meant to target specific users with ads specially selected to meet their profiles. When behavioral advertising networks create age-related profiles to target ads to children, they should not be able to shield themselves from COPPA.[10] Behavioral advertising networks earn profits from their ability to

---

[8] Children's Online Privacy Protection Rule, Supplementary Information, 64 Fed. Reg. 59888 at 59892 (Nov. 3, 1999) (codified at 16 C.F.R. § 312).

[9] *Id.*

[10] *See* The Institute for Public Representation, et al. Public Comment no. 33 on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Act Through the Children's

micro-target to demographic groups and when those groups are children, networks should acquire parental permission before collecting personal information.

Additionally, concerns about data security become even more salient for children's information. The process of targeting advertisements requires the extensive collection of data. The existence of such large data sets poses significant risks for costly breaches that expose children's personal data to those with malevolent intentions. In the context of children, behavioral tracking poses heightened risks, as data about specific interests and browsing patterns could be misused to gain children's trust and exploit their vulnerabilities. Providing parents with the ability to limit the collection and storage of data about their children (including their interests and browsing habits) falls precisely within COPPA's mandate.

4. Rejection of the E-Sign Consent Mechanism in § 312.5:

The proposed amendments on the use of e-signatures for parental consent appear to be inconsistent with the Electronic Signatures in Global and National Commerce Act ("E-SIGN Act").[11] The proposed amendment rejects the validity of an e-signature and takes the position that e-signatures do not adequately "confirm the underlying identity of the individual signing the document."[12] The E-SIGN Act, however, recognizes e-signatures as legally valid. Indeed, after passage of the E-SIGN Act in 2000, the FTC issued a report to congress stating that the benefits of allowing e-signatures to bind businesses-to-consumer contracts outweighed the burdens that came along with them.[13]

While an accurate parental verification mechanism is necessary for COPPA to achieve its goals, the FTC has not articulated any distinction as to why this use of e-signatures fails to properly authenticate the signing party in comparison to other uses of e-signatures and how this can be treated differently under E-SIGN.

In addition, as one recent study has shown, many parents wish to enable their children to use sites which collect personal information, even going so far as to help their children circumvent terms of service which prohibit child users.[14] For such parents, the inability to use familiar and simple e-signatures to grant permission under COPPA may well represent a hindrance on their ability to assert parental authority.

5. The Establishment of Standards for Data Retention in § 312.10:

The proposed amendments address data retention and deletion and would allow operators to retain personal information "for as long as is reasonably necessary to fulfill the

---

Online Privacy Protection Rule (June 30, 2010) (Arguing that when advertisers make claims that they can target ads to children, they should be deemed to have actual notice that users are children).

[11] Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified at 15 U.S.C. § 7001 *et seq*.).

[12] Children's Online Privacy Protection Rule, 76 Fed. Reg. at 59818 (proposed Sept. 27, 2011).

[13] Federal Trade Commission, Report to Congress on the Electronic Signatures in Global and National Commerce Act: The Consumer Consent Provision in Section 101(c)(1)(C)(ii) (June 27, 2001) *available at* http://www.ftc.gov/os/2001/06/esign7.htm.

[14] danah boyd, et al., *Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act',* 16 First Monday 11 (2011) *available at* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075.

purpose for which the information was collected."[15] This proposed restriction is overly permissive. The proposal offers no guidance as to what may be the permissible justifications for data retention. This creates an overly open-ended retention period. Operators would be able to avoid deleting data by citing purposes such as marketing or even the selling of customer lists which could inappropriately be used to justify indefinite storage. Without specific limitations on the length of time for data retention or on the purposes which can be used to justify that retention, the current proposal offers no effective guidelines on the appropriate storage duration periods.

To address this problem, the FTC should set a specific limit on how long data can be held before it must be deleted. For example, personal information collected under COPPA should be deleted no later than 18 months after a user's last visit to a site. Starting the data retention clock at the user's most recent point of contact rather than at the time the information was collected provides operators with needed flexibility to retain information for active users. After 18 months, if a user has not visited or contacted a site, operators should have little to no need to retain their personal information- even if it was once used for functional, internal purposes. Further, because children's tastes and interests shift and evolve frequently as they mature, it is unlikely that many sites will hold child users' interest for longer than 18 months. In addition, the FTC should make clear that when users actively take steps to close their accounts (rather than passively abandoning them), their personal information should be deleted immediately.

Allowing operators to self-define how long they will hold user information undermines the purpose of this important new addition to COPPA. Without a set limitation, operators can easily exploit the proposed rule change to keep children's data indefinitely.

[15] Children's Online Privacy Protection Rule, 76 Fed. Reg. at 59829 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312).