

Morrison & Foerster Client Alert.

August 3, 2012

FTC Proposes Further Significant Changes to Its COPPA Rule

By Julie O'Neill

On August 1, 2012, the Federal Trade Commission ("FTC") proposed clarifications to its previously proposed revisions to its rule implementing the Children's Online Privacy Protection Act ("COPPA").¹ Although the FTC's stated goals are to clarify COPPA's scope and strengthen protections for children, as a practical matter, the FTC's proposals would generally continue its expansion of COPPA's coverage and obligations. Not only would the proposals sweep additional online services, such as ad networks and social network plug-ins, into the law's coverage, as well as codify an age-screening obligation for certain sites, but they would also eliminate the distinctions between "personal" and "non-personal" information—an outcome that raises issues even for companies that are not subject to COPPA because they do not target or collect personal information from children.

Specifically, as discussed in more detail below, the new revisions would:

- **Extend COPPA's coverage to services, such as ad networks and plug-ins, when they knowingly operate through a child-directed site or service;**
- **Require child-friendly but mixed-audience sites to age-screen all users before collecting any personal information;**
- **Include screen and user names in COPPA's definition of "personal information" only when they function as contact information; and**
- **Clarify the circumstances under which the use of a persistent identifier constitutes "personal information" and thereby triggers COPPA's obligations.**

The FTC is accepting comments on its proposals until September 10, 2012. It has indicated that it expects to publish a final rule this year.

* * *

¹ See our [alert](#) from September 2011 discussing those previously proposed amendments.

Beijing

Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels

Joanna Kopatowska 32 2 340 7365
Olivier Proust 32 2 340 7360
Karin Retzer 32 2 340 7364

Hong Kong

Eric Dickinson 852 2585 0812
Gordon A. Milner 852 2585 0808

London

Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles

Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York

Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Matthew R. Galeotti (212) 336-4044
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia

Daniel P. Westman (703) 760-7795

Palo Alto

Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco

Roland E. Brandel (415) 268-7093
Anna Ferrari (415) 268-6728
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo

Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazacki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiko Terazawa 81 3 3214 6585

Washington, D.C.

Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

Client Alert.

If adopted as currently drafted, the FTC's new proposed revisions would:

- **Specifically apply COPPA to services that are integrated into a child-directed site or service.** Such services could include, for example, advertising networks and social media plug-ins. Recognizing the logistical difficulties that such services face in controlling and monitoring the sites that incorporate their services, the FTC declined to apply a strict liability standard to them. Instead, it proposes to apply COPPA only if the service “knows or has reason to know” it is collecting personal information through a host site or service that is directed to children.²
- **Require certain mixed-audience sites to age-screen their users before collecting any personal information.** Historically, the FTC has not charged child-friendly mixed audience sites as “directed to children” because of the burdens compliance would impose on both sites and users.³ Instead, it has charged sites as “directed to children” only where it believed that children under 13 were the primary audience. The FTC now proposes to revise COPPA to reflect this enforcement approach. If the revisions are adopted, then: (1) a site or service that knowingly targets or has content likely to attract children under 13 as its primary audience must treat all users as children and provide notice and obtain consent before collecting any personal information from any user; and (2) a site or service that has child-oriented content appealing to a mixed audience, where children under 13 are likely to be an over-represented group, will not be deemed directed to children if, prior to collecting any personal information, the site or service age-screens all users. Because the site or service thus learns which users are under 13, it must obtain appropriate parental consent before collecting any personal information from those users and otherwise comply with COPPA with respect to them.
- **Clarify the expanded definition of “personal information.”** Under COPPA, the online collection of “personal information” from a child generally triggers an obligation to obtain parental consent. Last September, the FTC proposed to extend COPPA’s reach to a far wider swath of information collection practices by expanding its definition of “personal information.” For example, it proposed modifying the definition to include persistent identifiers and screen or user names, other than where such identifiers or names are used “to support internal operations.” In response to the comments it received, the FTC proposes further revisions to those definitions:

Screen or user name: So as not to preclude sites from using screen and user names in place of individually identifiable information (a privacy-friendly approach), the FTC proposes to replace its prior proposal with a definition that treats user or screen name as “personal information” only when the name rises to the level of “online contact information,” such as an email address, an instant messaging identifier, or any other similar identifier that permits direct contact with the user. This proposal is more business friendly than the original proposal, as, if adopted, it would permit many sites and services to continue to use user or screen names without triggering COPPA’s obligations.

Persistent identifiers:⁴ As noted above, in September 2011, the FTC proposed adding to the definition of “personal information” a persistent identifier, “where [it] is used for functions other than or in addition to support for the internal operations of the site or service.” Many commenters objected to the proposal, saying that such information is

² The FTC explained that it is not imposing a duty on such services to monitor or investigate whether their services are incorporated into child-directed properties. It noted, however, that such services will not be free to ignore credible information brought to their attention indicating that such is the case.

³ The FTC has pursued such sites under COPPA when they have had “actual knowledge” of having collected personal information from children under 13. (COPPA applies to sites that are directed to children or that have actual knowledge that they are collecting personal information from children.)

⁴ “Persistent identifiers” include a customer number held in a cookie, an IP address, a device serial number, and a unique device identifier.

Client Alert.

Information collected from a device, not an individual, and should therefore not be treated as personal information that triggers COPPA's obligations. It is not surprising that the FTC disregarded this concern. In recent years, the FTC has repeatedly stated 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. If the FTC's proposals are codified, it is logical that the FTC will take the same approach in all contexts. For this reason, even companies that are not subject to COPPA should consider the potential ramifications of the proposed changes and consider submitting comments.

Commenters to the FTC's September proposal also objected that the proposed definitions of "persistent identifier" and functions that support "the internal operations of the site or service" were not sufficiently clear. The FTC has responded with new proposed definitions: one that expressly defines a "persistent identifier" as an identifier "used to recognize a user over time, or across different websites or online services;" and another that defines the activities that qualify as "support for the site's or service's internal operations" (and that therefore do not trigger COPPA's obligations) as solely those activities necessary to: (1) maintain or analyze the functioning of the site or service, (2) perform network communications, (3) authenticate users or personalize content, (4) serve contextual advertising on the site or service, (5) protect the security or integrity of the user, site, or service, or (6) fulfill a permitted request of a child. In its commentary to its September 2011 proposed revisions, the FTC included most of these as functions that "support the internal operations of the site or service." Here, it has added site personalization, analytics, and the performance of network communications to the list.

If these revisions are adopted as proposed, the definition of "personal information" would be triggered by—and consent would therefore be required for—any non-enumerated use of a persistent identifier, including for behaviorally-targeted advertising (as the FTC specifically noted in its commentary to the proposal). This proposal improves on its September 2011 proposal, in that it clarifies the circumstances under which the use of a persistent identifier would trigger COPPA's obligations. That said, it may still be difficult for sites and services to comply. Because there is no way to determine age from a persistent identifier, sites directed to children could not engage in retargeting or online behavioral advertising without first obtaining verifiable parental consent. For sites not directed to children but still subject to COPPA (because they knowingly collect personal information from children under 13), it is not clear how this restriction would apply in practice. As companies dealing with the EU's cookie requirements can confirm, obtaining consent prior to the use of a persistent identifier can be costly and disruptive.

* * *

On balance, the FTC's proposed revisions continue its theme of expanding COPPA's coverage and obligations. Not only does the FTC aim to extend those obligations to additional services, but it also codifies an age-screening obligation for child-friendly mixed audience sites. Moreover, the FTC has not backed away from its proposed extension of covered "personal information" to include information collected through certain uses of persistent identifiers. The new proposal improves on the earlier one in the sense that it clarifies the circumstances under which the use of a persistent identifier will trigger COPPA's obligations, but, as explained above, it may still be difficult for non-child-directed sites in particular to comply.

Client Alert.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's* A-List for eight straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "[*Global Employee Privacy and Data Security Law*](#)," or our free online Privacy Library, please visit: <http://www.mofo.com/privacy--data-security-services/> and "like" us on Facebook at <http://www.facebook.com/MoFoPrivacy>.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.