April 30, 2013

FTC Staff Updates its COPPA FAQs, Providing Crucial Guidance for Covered Operators

By Julie O'Neill and D. Reed Freeman, Jr.

Last week, the staff of the Federal Trade Commission ("FTC") issued crucial reading for operators of websites, apps, plug-ins, ad networks and other online services (together, "Services") that are subject to its recently revised rule implementing the Children's Online Privacy Protection Act ("Rule"): a much anticipated update of its COPPA FAQs.[1] Many of the 92 FAQs mirror those previously published by the staff, and most of the new FAQs draw largely from the FTC's Statement of Basis and Purpose issued with the final revised Rule. A few things, however, are new. While they do not address all of the issues businesses are facing as they prepare to come into compliance by the revised Rule's July 1, 2013, effective date, the FAQs provide valuable insight into how the staff interprets the revised Rule and how it thinks companies should comply.

Highlights are below.

- **The staff explains how operators should treat information that it collected prior to the revised Rule's effective date but that did not fall within the definition of "personal information" at the time it was collected (FAQ 4):**
    - *An operator must obtain parental consent "immediately" for already collected geo-location* because the inclusion of geo-location in the revised Rule's definition of "personal information" was a mere clarification of, and not a change to, the existing Rule.
    - An operator does not have to obtain parental consent for already collected *photos, videos and audio files*, but the staff recommends that, *as a best practice*, it either obtain parental consent or discontinue its use and disclosure of such materials.
    - An operator does not have to obtain parental consent for already collected *screen or user names*, but staff encourages that, *as a best practice*, it obtain parental consent, if possible. It also explains that a previously collected screen or user name is covered by the Rule if the operator associates new personal information with it after the revised Rule's effective date.

[1] The press release announcing the revised COPPA FAQs (including a link to the COPPA FAQs) is available at http://www.ftc.gov/opa/2013/04/coppa.shtm. The FAQs represent the views of staff and are not binding on the Commission. To learn about the FTC's recent revisions to the Rule, see http://www.mofo.com/files/Uploads/Images/130103-FTC-Issues-Substantially-Revised-COPPA-Rule.pdf.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
James R. McGuire (415) 268-7013
Daniel F. Muto (858) 720-7959
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Peter McLaughlin (212) 336-4290
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Virginia
Daniel P. Westman (703) 760-7795

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
L. 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
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

EUROPE

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

London
Ann Bevitt 44 20 7920 4041
Anthony Nagle 44 20 7920 4029
Caroline Stakim 44 20 7920 4055
David Varney 44 20 7920 4058

ASIA

Beijing
Gabriel Bloch 86 10 5909 3367
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

  - An operator does not have to obtain parental consent for an already collected *persistent identifier*, but if it associates new personal information with it after the revised Rule's effective date, then it must obtain parental consent (unless the collection falls within an exception, such as for the support of the Service's internal operations).

- **The staff takes the position that a Service that is directed to children but does not target children as its primary audience may not, after age-screening, completely block children from the Service.** Instead, it is the staff's view that *the Service must offer some content to children who identify as under 13*. This is new and flows from the Rule revision that permits such a Service to age screen users so that it may treat those who are under 13 differently from those who are older (rather than having to treat all users as children under 13, as the Rule generally requires of Services "directed to children"). Although neither the COPPA statute itself nor the revised Rule imposes an obligation on such a mixed audience Service to affirmatively provide content for those who identify as under 13, the staff's apparent theory for this requirement is that such a Service may not completely block children because it is directed to children and will therefore, presumably, know that it will attract children, including those who return after having been age-blocked.[2] (FAQs 36, 38, 53) It is not clear from the FAQs what the staff believes that such a Service *must do*—perhaps offering a minimum of content would suffice—only what such an operator apparently *cannot do*, which is to block age-screened under-13s altogether. This is new, untested and apparently unsupported in the Rule. Moreover, the staff's theory seems to require some evidentiary burden in any enforcement action. It may be revised in coming months. In the meantime, though, this is the staff's enforcement position.

- **The staff provides app operators with guidance on providing notice and obtaining verifiable parental consent.**
  - An app's *privacy policy* does not have to be posted at the point of download, such as in the app store, but such posting is recommended *as a best practice*. (FAQ 30)
  - *If an app will collect personal information as soon as it is downloaded*, the operator should provide direct notice and obtain parental consent at the point of purchase, or it should insert a landing page to do so before the download is complete. (FAQ 30)
  - *An operator may not rely on a parent's app store account number or password*, without some other indicia of reliability, to meet the Rule's consent requirements. The staff explains that this information, alone, does not provide sufficient assurance that the person entering the information is the parent and not the child. (FAQ 66)

- **The staff addresses an operator's obligations with respect to the collection of personal information by third parties from the operator's users.**
  - *The operator is not required to inform third parties of the child-directed nature of the Service*, but the staff recommends that it signal this to the third party because the operator is strictly liable for the collection of personal information from its users, including by a third party. The operator may arrange with the third party to provide adequate COPPA protections. (FAQ 40)
  - *An operator must inquire into the information collection practices of every third party that can collect information via the operator's Service*. The operator can assess its compliance obligations only if it has this information. (FAQ 42)

- **The staff provides guidance on how the revised Rule applies to photos submitted by children, a new category of "personal information" under the Rule.**
  - *A feature allowing children to submit photos* is subject to the Rule unless the operator prescreens them prior to posting and deletes any personal information contained in them, including images of children and geo-location metadata. (FAQ 44)

[2] The staff does not extend this obligation to general audience Services that age screen.

  - Compliance is not necessary *if an operator blurs the facial features of children in photos* before posting and removes any other personal information, including geo-location metadata. (FAQ 45)
  - The operator of an app does not "collect" personal information—and therefore does not trigger the Rule—*when the app interacts with a photo that is stored on the user's device* but is never transmitted to the operator. (FAQ 47)

- **The revised Rule requires an operator to take reasonable steps to release children's personal information only to service providers and third parties that are capable of maintaining its security and provide assurances they will do so. The staff believes this requires an operator to:**
  - Determine what the service provider or third party's practices are for maintaining security and confidentiality and preventing unauthorized access or use;
  - Expressly address expectations for treatment of the children's personal information in its contracts with the service provider or third party; and
  - Use reasonable means, such as periodic monitoring, to confirm that the service provider or third party is maintaining the security and confidentiality of the information. (FAQ 82)

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. 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 nine 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.