Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC's New Children's Privacy Guidance: 4 Traps To Avoid

Law360, New York (April 30, 2013, 12:11 PM ET) -- With the release of long-awaited guidance on the Federal Trade Commission's revised children's privacy rule, companies are scrambling to bring their websites, mobile applications and other online services into compliance before the July 1, 2013, deadline.

The guidance, which the FTC provided in over 90 frequently asked questions, clarifies amendments to the Children's Online Privacy Protection Act rule, which the FTC adopted last December. The FAQs provide greater certainty on how staff plan to apply the revised COPPA rule in an online environment where multiple parties collect data through a single site or platform. For example, the FAQs reiterate that third-party plugins can use persistent identifiers collected through a child-directed site or service to support the internal operations of the site or service, as well as the plugin itself.

However, the FAQs also identify some traps that easily could be missed by a company struggling to implement the changes over the next 60 days. We highlight four of these potential traps below.

1) Collecting Precise Geolocation Information Without Parental Consent

It is now common to be asked whether you want to allow a mobile application to access your location information before installing the app. While this "opt-in" consent is sufficient for adults, the FAQs clarify that "it is not sufficient to provide such notification and choice to the child user" because COPPA requires consent from a parent or legal guardian. Consequently, mobile app developers who direct their services to children or that have actual knowledge that a user is under the age of 13 must go beyond the standard opt-in consent process and get verifiable parental consent before collecting precise geolocation data. If you have collected geolocation information without obtaining parental consent, the FAQs state that you must seek parental consent immediately.

2) Blocking Children from Participating Altogether on Child-Directed Sites and Services

Under the revised COPPA Rule, the FTC created a new category of child-directed sites and services that do not target children as their "primary" audience. These child-directed sites and services may use neutral age screens to differentiate between users for purposes of complying with COPPA's notice and parental consent requirements. The FAQs go one step farther, however, by clarifying that these child-directed sites and services may not block children from participating in the site or service altogether.

Significantly, the FAQs explain that the operator of a site or service may offer different activities to different users depending on age. This suggests that an operator is permitted (but is not required) to allow teens and parents to participate in activities that allow the sharing of personal information, while children under 13 years old may be blocked from these activities as long as they are able to participate in other, non-interactive portions of the site or service.

3) Combining Existing Persistent Identifiers With New Information After July 1, 2013

Consistent with the approach it took when implementing the COPPA rule back in 1999, the FTC staff determined that the new COPPA rule should not be interpreted to cover information collected prior to its effective date. Consequently, because persistent identifiers were not covered under the original COPPA rule unless they were combined with personal information, operators are not required to obtain parental consent for persistent identifiers that were collected prior to July 1, 2013, and that were not combined with personal information.

However, if after July 1, 2013 (the date the new COPPA rule takes effect), an operator continues to collect the persistent identifier or combines the previously collected persistent identifier with new information, COPPA will be triggered and the operator must provide parents notice and obtain parental consent unless an exception applies.

4) Companies Collecting Personal Information from Children in Schools Must Provide Parents Notice and Obtain Consent Before Using the Data for Commercial Purposes

The FAQs emphasize that vendors of educational cloud computing services and other online services in schools must provide schools and parents notice "regarding what data is collected from children, how it will be used, and with whom it will be shared." Where the child's personal information will be used for the vendor's own commercial purposes, the vendor must obtain parental consent. To ensure COPPA compliance, the FAQs encourage schools to ask their vendors a number of questions about how they collect, use, disclose and protect student data, including whether children's personal information is used for online behavioral advertising or building user profiles for unrelated commercial purposes.

--By Matthew DelNero and Lindsey Tonsager, Covington & Burling LLP

Matthew DelNero is a partner and Lindsey Tonsager is an associate in Covington's Washington, D.C., office.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.
