

FTC's Child Privacy Tweaks Bring Ad Networks Under Scrutiny

By **Allison Grande**

Law360, New York (August 01, 2012, 10:45 PM ET) -- The Federal Trade Commission on Wednesday proposed revisions to its children's online privacy rule that would require services that choose to integrate with child-directed websites to enact more stringent safeguards, a move attorneys say will for the first time draw certain advertisers and mobile apps into the regulation.

In a Federal Register notice, the FTC reopened to public comment its efforts to update the Children's Online Privacy Protection Act rule, after making several modifications to definitions such as "operator" and "personal information" to clarify the scope of the rule in response to the 350 comments the agency received on its original proposal to revise the regulation in September.

The latest changes sweep third parties such as advertising networks or downloadable software kits that interact with child-directed websites into the rule's requirements by expanding the definition of "operator" to include these entities and tweaking the definition of "website or online service directed to children" to clarify that services are covered by the rule when they know or have reason to know that they are collecting information through a child-directed website or online service.

"The commission now believes that the most effective way to implement the intent of Congress is to hold both the child-directed site or service and the information-collecting site or service responsible as cooperators," the agency's notice said. "Online services whose business models entail the collection of personal information and that know or have reason to know that such information is collected through child-directed properties should provide COPPA's protections."

These tweaks not only supplement existing information-collection safeguards for children, but they also respond to growing concerns over the way companies are using emerging technology such as behavioral advertising and mobile apps to gather data about children, according to attorneys.

"These changes are outside the original intent of the regulation, which was to address mobile computing and social media data collection issues," Morgan Lewis & Bockius LLP partner Gregory Parks told Law360 on Wednesday. "But as the FTC was studying these issues, it unexpectedly seized on the degree to which advertisers use identifiers on devices and stationary computers to track information about users. The latest revisions confirm the frequent interpretation of COPPA that advertisers should also be subject to the rule."

This expansion of liability to third-parties applies not only to online websites, but also to the growing world of mobile apps, attorneys noted.

“There are more instances now than a couple of years ago where companies need to look and see if they have obligations under COPPA in the mobile space,” Holland & Knight LLP data privacy and security team co-chair Steven Roosa said. “There's no carve-out for mobile in these regulations, and it's clearly an area of increasing focus for the FTC.”

Tying these third-parties' use of mobile apps into the regulation also reflects the public's mounting concern over the use of this technology by children, according to Cooley LLP privacy practice group co-chair Susan Lyon.

“Parents and others are recognizing that children more and more are using mobile applications and devices,” she said. “And because that's happening, the rule needs to be updated to address this issue.”

To deal with the presence of third-parties on child-directed services in both the online and mobile space, the FTC wants to require companies to gain consent if they knowingly target children under 13, a requirement that Reed Smith LLP partner John Feldman notes is not far from the current recommendations advanced by the Children's Advertising Review Unit.

“The self-regulatory practice for many years at CARU has been that if a website or referring medium is of interest to children, then companies should assume that children might be coming to their site if they link from that website and they should put up an age gate,” he said. “What the FTC is doing is trying to close the gap between the practice that is prevalent at CARU and the COPPA rule, which is interesting because, unlike with the self-regulatory body, when you violate an FTC rule, there are substantial penalties for that.”

The FTC's proposal causes additional concern because it goes beyond this standard by not only including services that knowingly target or are likely to attract children under 13, but also those that are “likely to attract ... a disproportionately large percentage of children under age 13 as compared to the percentage of such children in the general population,” Feldman added.

“It's not clear if the FTC has effectively differentiated and flushed out the various possibilities along this continuum of what constitutes a service directed to children,” he said.

This potentially broad definition is likely to encompass more service providers than before into the regulation, setting up a new dynamic between website providers and third-party services, according to Feldman.

“The FTC is trying to get as many people involved in the regulation as possible,” he said. “Because the website operator and the service provider who puts the link on the website will have shared responsibility, they'll be looking at each other a lot more, and their contracts are going to reflect that with more monitoring and auditing by the website operator.”

This expanded regulation could also result in the unwillingness of ad networks to get into the market, Hogan Lovells' privacy and information management practice group director Christopher Wolf said.

“It remains to be seen whether the extension of the rule will discourage social app developers and online analytic and targeting companies that won't want to run the risk of running afoul of the expanded rule and therefore stay away from certain sites and markets,” he said.

While the FTC's latest revisions expand the regulation's reach, it also narrows the previously broad definition of "personal information" by exempting nonpersonalized activities such as the use of persistent identifiers for authenticating users, the use of cookies to maintain user preferences and the serving of contextual advertisements from the rule's stringent consent requirements. The tweaks make clear that a persistent identifier will be considered personal information where it can be used to recognize a user over time, or across different sites or services, and where it functions like an email address.

But although the change clarifies the circumstances under which the use of a persistent identifier will trigger the rule's obligations, it may still be difficult for non-child-directed sites to comply, according to Julie O'Neill of Morrison & Foerster LLP.

"As companies dealing with the European Union's cookie requirements can confirm, obtaining consent prior to the use of a persistent identifier can be costly and disruptive," she said.

These proposed revisions, which will be open for public comment until Sept. 10, will most likely be integrated into a final rule with other previously recommended revisions — including the elimination of the popular email consent mechanism and increased oversight of COPPA safe harbor programs. But regardless of how the final regulation pans out, Lyons viewed it as a positive that the FTC elected to propose further modifications based on the public's feedback before issuing a binding rule.

"The purpose of having comments is to understand what the industry's concerns are, so it's a really good thing that the FTC recognized that and proposed additional rules," she said. "The industry is really hungry for information about how to actually comply with these rules given all of this new technology, and while some of these rules may be challenging for companies, others will most likely welcome the clarity they provide."

--Editing by Elizabeth Bowen and Andrew Park.

All Content © 2003-2012, Portfolio Media, Inc.