

FTC Updates COPPA FAQs to Address New Rules

APRIL 30, 2013

The FTC has updated its Frequently Asked Questions for complying with the Children's Online Privacy Protection Act Rule (COPPA) as a follow up to recent revisions to the Rule. As we previously reported, changes to the COPPA Rule go into effect on July 1, 2013. The amendments to the Rule did not alter the fundamental structure: Those who operate a website or online service directed to children under 13 must still give notice to parents and obtain their verifiable consent before collecting, using, or disclosing personal information from children under 13. Certain important changes – such as the addition of new categories of “personal information” – have caused the FTC to embark on the FAQ update. While the FAQ does answer some questions, it certainly doesn't answer all. For example, FAQ #41 indicates that in some circumstances, companies engaging in online behavioral advertising on their websites will need to notify parents and obtain parental consent. It just is not entirely clear from the FAQ when those circumstances exist (and when such notice/consent is unnecessary). Even with these new FAQs, companies will thus still need to review the amended Rule carefully. For example, with respect to OBA, the modified Rule indicates that companies with sites directed to children – or knowingly collecting information from children – must get parental consent before collecting personally identifiable information, which includes persistent identifiers used to serve behaviorally targeted ads. So websites may need to go back and re-evaluate whether they are covered by COPPA (i.e., directed to children, or knowingly collecting information from children). The FAQs also remind companies in the OBA space that they will need to engage in due diligence to determine what their vendors are doing, since the amended Rule holds companies liable for the collection of information that occurs on or through your sites and services. This same diligence holds true for mobile apps: “As the operator of a child-directed app, you must conduct an inquiry into the information collection practices of every third party that can collect information via your app.” With respect to apps, the FAQs also give some direction about obtaining parental consent, noting that if personal information will be collected from a child immediately after the app is downloaded, then parental consent will be needed before the download (for example, at the point of purchase). Again, there is not in the FAQ clear direction on how that consent must be obtained, with the FTC instead leaving it up to the industry to develop appropriate mechanisms. These might include, for example, offline consent procedures (but would not include, the FTC specifically indicates in FAQ #66, relying on the parent's app store account). The FTC also reminds companies to look at what the app does to determine if consent is needed. For example, if an app permits a child to upload and decorate photos – but the company does not send the photos from the device to the company – then information has not been “collected.” (And thus, consent would not be necessary.)

TIP: The FAQs provide some direction on how to address tricky topics like OBA on child-friendly websites and the operation of mobile apps for kids. Not all of the answers a company might need are included in the FAQs, however. Thus while companies should review these carefully, they will still need to go back to the amended Rule and analyze it against current business practices to ensure compliance. While July 1st is the current date for compliance, 18 industry groups (including the US Chamber of Commerce and the Direct Marketing Association) have asked the FTC to delay this date to give companies more time to adapt to unanticipated changes created by the Final Rule.

This tip has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.

3 Min Read

Related Topics

Mobile Privacy

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.