Privacy Alert: COPPA Amendment Impacts Apps, Ads and Social Networks

MADELINE ZAMOYSKI AND TYLER NEWBY

Fenwick
FENWICK & WEST LLP

After a two-year comment process, the Federal Trade Commission adopted its long-awaited amendments to the Children's Online Privacy Protection Rule in December 2012. The amendments, which go into effect July 1, 2013, clarify, supplement and revise the Rule issued under the Children's Online Privacy Protection Act (COPPA) in many areas, and have particularly important implications for mobile application developers, advertising networks and social networking services.

COPPA imposes notice and verifiable parental consent requirements on the operators of websites or online services that are directed toward children under the age of 13 or for operators who have actual knowledge they are collecting or storing "personal information" from children under the age of 13. Operators are prohibited from conditioning a child's participation in an activity upon disclosure of unnecessary personal information and required to take reasonable steps to secure any personal information collected from children.

On a high-level, the amended Rule (i) addresses new COPPA compliance requirements for plug-ins and advertising networks; (ii) adds new categories of protected personal information, including persistent identifiers and location information; (iii) supplements the definition of "directed to children" to add criteria and clarify when age-screens are appropriate; (iv) clarifies the required language for direct notices to parents; (v) supplements the consent mechanisms available to operators (and retains "email-plus"); (vi) clarifies safe-harbor processing requirements and adds reporting requirements for safe harbor providers; and (vii) expands COPPA's security requirements to third parties that receive information from operators.

Who Is Impacted?

Operators of websites and online services subject to COPPA now face strict liability for the conduct of third party service providers (including plug-ins or ad-networks) that collect information through the operator's website or online service. This is, in part, a result of the amendment providing that personal information is collected or maintained on behalf of an operator when it is (i) collected or maintained by an agent or service provider of an operator; or (ii) the operator benefits by allowing another person to collect personal information directly from users of such operator's website or online service.

Under the amendment, third party service providers, e.g., plug-in providers and ad-networks, are liable for compliance with COPPA when they have actual knowledge of the collection of personal information directly from users of a child-directed site or service. In addition, third party service providers will be liable for compliance if a portion of their services become child-directed, e.g., if a behavioral advertising network offers age-based advertising segments to target children under 13. The FTC suggested that actual knowledge will be met in cases where (i) a child-directed content provider directly communicated the child-directed nature of its content to the other online service, or (2) a representative of the online service recognized the child-directed nature of the content.

Expanded Definition of "Personal Information"

The amended Rule both clarifies and expands the types of information considered to be "personal information" under COPPA, including (i) screen names (where it functions as online contact information); (ii) photo, video and audio files that contain a child's image or voice; (iii) geolocation data; and (iv) persistent identifiers that can be used to recognize a user over time and across different websites or online services, such as an IP address, or unique device identifier.

Under the amendment, persistent identifiers do not need to be coupled with other personal information to be considered personal information. To balance this expansion, the FTC clarified that if an operator collects a persistent identifier for the sole purpose of providing support for its internal operations, then the operator is not required to provide notice or obtain prior parental consent for such collection and use. In addition, the FTC expanded "support for internal operations" to include frequency capping of advertising and legal or regulatory compliance. The amended Rule also establishes a voluntary process where entities may submit additional

proposed uses as "internal operations," subject to public consideration and comment, which the FTC will respond to within 120 days of submission.

Directed to Children

The FTC added several provisions to the definition of "directed to children", including (i) addition of musical content, presence of child celebrities and celebrities that appeal to children to the list of criteria used to determine whether a website or online service is "directed to children"; (ii) an actual knowledge standard for a plug-in, ad network or other property; and (iii) provisions outlining when an operator is permitted to age-screen to differentiate among users.

Under the amended Rule, a website or online service may meet the criteria used to determine whether it is directed to children, but if the website or online service does not target children as its primary audience, it will not be deemed "directed to children" if it (i) collects age information before collecting any personal information, and (ii) prevents the collection, use or disclosure of personal information of visitors that self-identify under 13 years of age. If a website or online service is directed to children and targets children as its primary audience, it must presume all visitors are children.

Parental Notice

The amendments clarify the specific information required in the direct notice to parents under COPPA, which includes: (i) that the operator collected the parent's online contact information (and any other information, if applicable) in order to obtain the parent's consent; (ii) that the parent's consent is required for the collection, use or disclosure of such information; (iii) any additional items of personal information that the operator intends to collect from the child or potential opportunities for disclosure, if the parent provides consent; (iv) a hyperlink to the operator's privacy policy; (v) the means by which a parent may give verifiable consent; and (vi) that if the parent does not provide consent within a reasonable time, the operator will delete all information it has collected so far.

With respect to an operator's privacy policy, the amendments remove the requirement for an operator to recite that it is restricted from conditioning a child's participation on unnecessary collection of information, and explicitly requires a link to the online notice on the landing page or home screen of the children's area of a website or child-direct app.

Verifiable Parental Consent

The amendment adds the following methods to the non-exhaustive list of approved methods for obtaining verifiable parental consent: (i) electronic scans of signed consent forms and video conferencing; (ii) collecting government issued identification and checking identification against a database of such information (provided such information is deleted after verification); (iii) monetary transaction on a credit card, debit card, or other online payment system that notifies or records each discrete transaction to the primary account holder.

Despite the FTC's initial proposal to eliminate the sliding scale approach for parental consent (also known as "email-plus"), the final amendment retains the email-plus option for information collected and used solely for internal purposes.

The amendment institutes a new voluntary approval process, where entities can propose a new consent mechanism for approval along with a statement of how the consent mechanism complies with COPPA, and, after public review and comment, the FTC will provide a written determination within 120 days of filing.

The FTC adopted provisions that allow operators participating in an FTC-approved safe harbor program to use any parental consent mechanism deemed by the safe harbor program to meet the general consent standard of 312.5(b)(1).

The Rule initially provided for five circumstances under which operators were not required to obtain parental consent prior to collection and use of certain information. The final amended Rule has some small changes, including: (i) allowing operators to collect parental contact information to provide voluntary notice to and subsequent updates about the child's participation in a website or online services; (ii) modifying the multiple use exception to allow for collection of the child and parent's online contact information and striking the collection of postal address under this exception; (iii) extending the information allowed under the child safety exception

to include the parent's name and online contact information in addition to the child's name and online contact information; (iv) allowing operators to collect persistent identifiers, and no other personal information, where it is used solely to provide support for the internal operations of the website or online service; (v) allowing an operator to collect a persistent identifier, and no other personal information, from a user who affirmatively interacts with the operator and whose previous registration with the operator indicates he or she is not a child (e.g., clicking on a plug-in for an online service where the user has self-identified as 13 or over) provided that the interaction must be active and the exception does not apply if the online service passively collects personal information from the user while he or she is on another site or service.

Safe Harbor

The FTC adopted additional criteria for approval of a self-regulatory program and incorporated additional provision to clarify the process for requesting approval. In addition, the FTC instituted certain reporting and record keeping requirements for safe harbor programs that require such programs to provide annual reports on compliance, but the reports may discuss compliance in aggregate.

Security

The amended Rule requires operators to take reasonable steps to release children's personal information only to service providers and third parties that are capable of maintaining the confidentiality, security and integrity of such information and provide assurances that they will do so. This new requirement does not require operators to ensure compliance, but does require them to inquire about the entities' data security capabilities and, either by contract or otherwise, receive assurances about how the information will be treated. In addition, the amended Rule limits retention of personal information for "only as long as is reasonably necessary to fulfill the purpose for which the information was collected" and requires an operator to use reasonable measures to protect such information in connection with its deletion.

For further information, please contact:

Madeline A. Zamoyski, Associate,
Intellectual Property Group
mzamoyski@fenwick.com, 650.335.7639

Tyler G. Newby, Partner, Litigation Group
tnewby@fenwick.com, 415.875.2495