September 21, 2011

On September 15, 2011, the U.S. Federal Trade Commission (FTC) issued proposed amendments to the rules implementing the Children's Online Privacy Protection Act (COPPA). The COPPA statute and rules cover online sites and services that collect personal information and direct activity toward children under the age of 13. They also apply to operators of general audience sites and online services that have actual knowledge that they collect information from children. In the background to its proposed rules, the FTC noted "the rapid-fire pace of technological change" since its last review, including "an explosion in children's use of mobile devices" as prompting its proposals. Accordingly, the proposed amendments, in part, confirm COPPA's application to mobile sites and services and expand the definition of personal information to include mobile data such as location data and mobile device identifiers.

Mobile activities = online service

The FTC affirmed application of the term "online service" as currently defined to include mobile services. In support of its position, the FTC noted a "consensus" by commenters and roundtable participants that the COPPA statute and rule are "device neutral." The FTC also described the phrase, "website located on the Internet," as broadly understood to cover content accessible through a browser on a mobile device. Based on this perceived recognition, the FTC declined to modify the definition of the term "online service" stating that it already broadly covers any service available over the Internet, or that connects to the Internet or a wide-area network.

The FTC in its comments, provided the following useful examples of mobile activities that it would consider to be "online services":

- Internet-enabled location based services.
- Mobile applications that allow children to:
  - play network-connected games,
  - engage in social networking activities,
  - purchase goods or services online,
  - receive behaviorally targeted advertisements,
  - interact with other content or services, or
  - send text messages from web-enabled devices and traverse the Internet for at least a portion of the message routing.
- Retailers' premium texting and coupon texting programs that register users online and send text messages from the Internet to users' mobile phone numbers.

In noting that certain texting activities would be considered online services, the FTC cited CTIA, the Wireless Association's comments that "SMS and MMS text messages cross wireless service providers' networks and short message service centers, not the public Internet, and therefore that such services are not Internet-based and are not ‘online services.'" The Commission in its footnote to its comment agreed, "that where mobile services do not traverse the Internet or a wide-area network, COPPA will not apply."

"Personal information" definition changes

Other changes of significance to mobile services include the FTC's proposed expansion of the definition of personal information. In particular, among the changes proposed by the FTC are greater application of COPPA to persistent identifiers and explicit coverage of certain geolocation information.

Persistent identifiers (device IDs)

Currently, persistent identifiers must be associated with individually identifiable information to be considered personal information. Under the proposed changes, "device serial numbers," "unique device identifiers" (which presumably would include mobile serial numbers and mobile device IDs) and other persistent identifiers alone would be personal information. The proposed definition effectively exempts use of persistent identifiers for "internal operations" but would cover "an identifier that links the activities of a child across different websites or online services." Thus, under the proposed definition, "an advertising network or analytics service that tracks a child user across a set of websites or online services, but stores this information in a separate database rather than with the persistent identifier, would be deemed to have collected personal information."

Use of persistent identifiers for purely internal purposes such as "user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft" would not be deemed to be collection of personal information. Of significance to the mobile industry, however, is that the term "internal purposes" is limited only to those of a "website or online service." This creates ambiguity as to the application of the exception to internal operations relating to telecommunication systems supporting non-Internet functions such as non-VOIP voice communications, handset operations unrelated to Internet services and text messages and other data sent across a wireless service providers' networks.

Geolocation data

The Commission also proposes a stand-alone category of geolocation information under its definition of personal information. Under the proposed rule geolocation data that provides information at least equivalent to "physical address" would be personal information. Acknowledging that geolocation information that identifies the name of a street and city or town is already covered under existing paragraph (b) of the definition of "personal information," the FTC reasons that geolocation information may be presented in a variety of formats and may be more precise than street name and name of city or town. The FTC rejected arguments that geolocation information identifies a device and not an individual.

Multiple operators

The Commission also revises its notice requirements to include a requirement for "multiple operators" on a single website or online service to each identify themselves. The concept of multiple operators is potentially significant for mobile advertising, mobile marketplaces and software development kits (SDKs) for use and incorporation into mobile apps all of which tend to involve multiple parties. No guidance is provided or proposed, however, as to what would cause a third party to be considered an additional operator of a website or online service. The FTC mentions parenthetically one example of a mobile application and an advertising network that collects information from within the application. No mention is given as to whether both the mobile application and the advertisement need to be directed toward children or whether both might be operators simply because either the mobile application or the advertisement is directed toward children. If the latter, this raises questions regarding whether parties have an obligation to conduct due diligence on the activities of the other party and the effect, if any, of contractual prohibitions on targeting children.

Other notable comments and proposals relating to application of COPPA:

- The FTC declines to advocate a change to the definition of children to include teens citing potential impact on free speech rights.

- The FTC declines to advocate a change to the actual knowledge standard applicable to general audience sites.
- Changes the term "requesting that children submit personal information online" to "requesting, prompting, or encouraging a child to submit personal information online" to clarify that the Rule covers when an operator mandatorily requires information, and when an operator merely prompts or encourages a child to provide such information.
- Replaces the "100% deletion standard" under the blogging exception with a "reasonable measures" standard "whereby operators who employ technologies reasonably designed to capture all or virtually all personal information inputted by children should not be deemed to have 'collected' personal information." (Under the current COPPA exception an operator may allow children to publicly post to online services such as chat forums and social networking services only if posts are screened and if "all individually identifiable information" is deleted.)
- Revises the definition of "collects or collection" to "clarify" that it includes any passive tracking of a child online, without the limiting reference of any particular type technology to do so (previously, the category specified "an identifying code linked to an individual, such as a cookie.")
- Expands the exemption of personal information collected for "support for the internal operations of a website or online service," to include "activities necessary to protect the security or integrity of the website or online service" recognizing "operators' need to protect themselves or their users from security threats, fraud, denial of service attacks, user misbehavior, or other threats to operators' internal operations."
- Amends the definition of "online contact information" to include specific examples of identifiers that permit direct contact: "an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier."
- Characterizes screen or user names as personal information if used for purposes beyond internal operations of a website or online service.
- Adds video and audio files containing a child's image or voice to the existing photos category of personal information.
- Declines to include date of birth, gender or Zip code to the definition of personal information but seeks comment on whether the combination of these data elements should be considered personal information and whether Zip + 4 is the equivalent of a physical address.
- Adds the following as additional factors the FTC will consider to determine whether a website or online service is directed toward children: musical content, child celebrities and celebrities that appeal to children.

Proposed requirements for sites and online services directed toward children or with actual knowledge of collection from children:

- Reverses guidance that information in direct notices may be truncated by providing a link to the online privacy policy and requires the online notice to be clearly labeled and prominently presented. Whether operators should be required to post a link to their online notice anywhere their mobile applications can be downloaded or purchased is presented as a question for comment.
- Revises the notice requirements to require operators to provide contact information, including at minimum the operator's name, physical address, telephone number and email address.
- Eliminates need for a privacy policy to state that an operator may not condition an activity on the child's disclosing more personal information than is reasonably necessary to participate (while keeping the actual, underlying prohibition).
- Recognizes electronic scans and video conferencing as means to obtain parental consent (but rejecting use of electronic signature and use of touch screen to obtain electronic sign and send citing ease with which a child could sign and return an online consent due to prevalence of mobile devices).
- Allows collection of sensitive information such as drivers license information and government identification to conduct verification provided that information is deleted following completion of verification.
- Requires actual monetary transactions be conducted to use a credit card as a means to proving parental consent.
- Eliminates the "sliding scale" or "email plus" method of parental consent currently permitted when information is collected only for internal use. The email plus method allows verifiable consent to be obtained through email from the parent plus some other

form of communication such as postal mail, phone, or delayed confirmatory email.

- Rejects proposals to use SMS text messaging as a means to obtain parental consent. The Commission cites the need for a statutory change as the Act currently only permits "online contact information" be used for such purposes.
- Requires reasonable measures to ensure that service providers use reasonable confidentiality, security and integrity procedures to protect children's data.
- Limits data retention to only as needed to fulfill the purpose for which the data was collected.

Comments to the proposed rules are due November 28, 2011.

For questions about this summary, or interest in submitting comments, please contact one of the attorneys listed above.

Key Contacts

Michael Rhodes San Francisco	rhodesmg@cooley.com +1 415 693 2181
Howard Morse Washington, DC	hmorse@cooley.com +1 202 842 7852