FTC ISSUES UPDATED FAQS ON AMENDED COPPA RULE

The Federal Trade Commission (FTC) recently issued updates to its frequently asked questions (FAQs) relating to the FTC’s amendments to the Children’s Online Privacy Protection Act (COPPA), which will take effect on July 1, 2013. Click here for a previously authored D&G Alert on this topic. In response to a request by industry organizations to reconsider the July 1st deadline, the FTC recently decided by unanimous vote to retain the implementation date for the COPPA amendments.

The eagerly-awaited document includes ninety-two FAQs, which cover a wide range of issues, including advertising networks, app and plug-in developers, mixed-audience sites, and child-directed sites. Below is a summary of some of the more important highlights.

GENERAL QUESTIONS ABOUT THE AMENDED COPPA

In addition to providing a general overview of COPPA, the FAQs answer one of the most important questions with respect to the COPPA amendments – the FTC’s position with respect to “legacy” information collected prior to the effective date of the amendments in the four new categories of information deemed to be personal information under the amended COPPA (i.e., geolocation information, photos or videos containing a child’s image or audio files with a child’s voice, or who have collected the newly covered screen or user names or persistent identifiers). According to the FTC, operators who have collected geolocation data and have not obtained parental consent must do so immediately. In contrast, operators who have collected photos or videos containing a child’s image or audio files with a child’s voice, or who have collected the newly covered screen or user names or persistent identifiers prior to the effective date, do not need to obtain parental consent (although the FTC encourages parental consent as a best practice). With respect to the latter two items, operators must obtain parental consent and COPPA is triggered if the operator associates new information with the previously collected screen or user name or if the operator continues to collect new information with a persistent identifier, such as the child’s activities on the website.

To the extent there was any doubt, FAQ 9 makes clear that COPPA applies to personal information collected online by operators of both websites and online services, and that the term “online service” broadly covers any service available over the Internet or that connects to the Internet or a wide-area network, including services that allow users to play network-connected games,

THE BOTTOM LINE

Advertising networks, app and plug-in developers, mixed-audience sites, and child-directed sites should carefully study the updated FAQs – and the COPPA amendments – and make certain that they are taking all steps necessary to ensure that they are in compliance by the July 1st deadline. Also, in addition to the FAQs described in this Alert, there are many other FAQs of importance, including a special section on COPPA and schools and COPPA Safe Harbor Programs.
engage in social networking activities, purchase goods or services online, receive online advertisements, or interact with other online content or services. Mobile applications that connect to the Internet, Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location-based services are also considered online services covered by COPPA.

FAQ 14 acknowledges that the amended COPPA will not prevent children from lying about their age when registering for general audience sites or online services whose terms of service prohibit their participation, and indicates that an operator of a general audience site or service that chooses to age screen its users in a neutral fashion may rely on the age provided by users, even if that age is, in fact, inaccurate. FAQ 14 adds, however, that if an operator determines that a particular user is a child under age 13, then COPPA’s notice and parental consent requirements will be triggered.

COPPA ENFORCEMENT

According to FAQ 18, if a website or app does not currently comply with COPPA, the operator must stop collecting, disclosing, and/or using personal information from children under age 13 until the website or online service is COPPA compliant. The operator also must review its information practices and online privacy policy, considering the information it collects, how it is collected and used, whether the information is necessary, whether there are adequate mechanisms for providing parents with notice and obtaining verifiable consent, whether there are adequate methods for parents to review and delete their children’s information, and whether adequate data security, retention, and deletion practices are in place.

PRIVACY POLICIES AND DIRECT NOTICES TO PARENTS

Several FAQs focused on operators’ obligations with respect to privacy policies and direct notices to parents after the effective date. FAQ 25 explains that a privacy policy for a children’s app may have to change to comply with the amended COPPA if, for example, the operator collects information from children that is now considered personal information under COPPA, but previously was not. The existing practice of listing the name and contact information of one operator who will respond to all parental inquiries is retained in the amended COPPA, provided that the names of all of the operators are also listed in this online notice (FAQ 26). The amendment to COPPA that defines “personal information” to include certain identifiers (such as a customer number held in a cookie, an IP address, a processor or device serial number, or a unique device identifier that can be used to recognize a user over time and across different websites or online services, even where the identifier is not paired with other items of personal information) will require an operator to disclose in its privacy policy and in its direct notice to parents its collection, use, or disclosure of such persistent identifiers. Disclosure is not required, however, where the operator collects no other “personal information” and persistent identifiers are collected on or through the site or service solely for the purpose of providing “support for the internal operations” of the site or service (FAQ 27).

APPS

Not surprisingly, a number of FAQs relate specifically to apps, as there had been a number of questions with respect to how apps can comply with COPPA. For example, FAQ 30 points out that, in connection with an app directed to children, the amended COPPA does not mandate that a privacy policy be posted at the point of purchase; rather, it requires that it be posted on the home or landing screen. This FAQ notes however, that there is “a substantial benefit” in providing greater transparency about the data practices and interactive features of child-directed apps at the point of purchase, and providing greater transparency is “encourage[d]” as a “best practice.”

Regarding the timing of direct notice to parents for apps directed to children, FAQ 34 clarifies that direct notice to parents must be sent prior to the collection of any personal information from the child, excluding the limited
circumstance in which an operator collects the parent’s online contact information for the sole purpose of sending the parent the direct notice. To that end, if a child-directed app is designed to collect personal information as soon as it is downloaded, it would be necessary to provide the direct notice and obtain verifiable consent at the point of purchase or to insert a landing page where a parent can receive notice and give consent before the download is complete.

Notably, FAQ 66 explains that a mobile app operator cannot rely on a parent’s app store account to serve as verifiable parental consent even if a credit card is attached to that account. It reasons that the “mere entry” of an app store account number or password, without other indicia of reliability (e.g., knowledge-based authentication questions or verification of government identification), “does not provide sufficient assurance that the person entering the account or password information is the parent, and not the child.”

**AD NETWORKS AND PLUG-INS**

Various FAQs relate specifically to advertising networks and plug-ins. For instance, FAQ 41 notes that an operator that wants to run ads on its child-directed websites and apps must explore certain issues before entering into an arrangement with any entity that provides advertising, including:

- **Is there a way to control the type of advertising that appears on the sites and services?** For example, can the operator stipulate and contract only for contextual advertising, and can it prohibit behavioral advertising or retargeting?

- **What categories of information will be collected from users on the sites and services in connection with the ads they are served?** Will persistent identifiers be collected for purposes other than support for internal operations? Will geolocation information be collected in connection with the ads served?

Depending on what advertising choices an operator makes, parental notification via the privacy policy and direct notice, as well as verifiable parental consent, may be required prior to delivering this advertising. In addition, FAQ 77 provides that both a child-directed website and a third-party plug-in that collects persistent identifiers from users of that child-directed site can rely on the amended COPPA’s exception for “support for internal operations” including, for example, site analytics.

By contrast, FAQ 79 states that the use of persistent identifiers by an ad network to personalize advertisements on websites is not considered “support for internal operations,” because the term “support for internal operations” does not include behavioral advertising.

**PHOTOS, VIDEO, AND AUDIO RECORDINGS**

Consistent with the industry trend to incorporate more photos, videos, and audio recordings in websites and apps directed to or accessed by children, several FAQs explicitly address these issues.

An operator that runs a moderated website directed to children, where all children’s submissions are prescreened to delete personal information before postings go live, must obtain parental consent if children are allowed to post photos of themselves – even if they may post no other personal information (FAQ 43).

FAQ 44 describes the steps that an operator must take to offer – without parental notice or consent – a child-directed app that would allow children to upload pictures of their favorite pets or places, but no personal information:

- Pre-screen the children’s photos to delete any that depict images of children or to delete the applicable portion of the photo, if possible;

- Remove any other personal information – e.g., geolocation metadata – contained in the photos prior to posting them through the app; and

- Ensure that any persistent identifiers are used only to support the internal operations of the app and are not used or disclosed to contact a specific individual or for any other purpose.

>> continues on next page
As FAQ 45 states, an operator of a site directed to children does not need to notify parents or obtain their consent if it blurs the facial features of children in photos before posting them on its website. The same is true for a site that has actual knowledge it has collected the photos from children. Before posting these photos, however, the operator also must remove any other personal information they contain, such as geolocation metadata, and ensure that it is not using or disclosing persistent identifiers collected from children in a manner that violates the amended COPPA.

GEOLOCATION DATA

Given that geolocation information is included as a new category in the amended COPPA’s definition of “personal information,” it should be no surprise that, as mentioned above, it is referred to frequently throughout the FAQs. An operator that collects geolocation information from users of its children’s app is covered by COPPA even if it does not use this information in any way, and thus must notify parents and obtain their verifiable consent prior to collection (FAQ 48).

Even where an operator gives users a choice to turn off geolocation information, parents still must be notified and the operator still must obtain parental consent (FAQ 49).

By contrast, because the amended COPPA covers “geolocation information sufficient to identify street name and name of city or town,” a children’s app that only collects coarse geolocation information, tantamount to collecting a ZIP code but nothing more specific, does not require notice to, or consent from, parents. However, FAQ 50 warns that the operator should be quite certain that, in all instances, the geolocation information collected is general and not sufficient to identify the street name and the name of the city or town. Consistent with the above, the collection of geolocation information through an app that takes the user’s longitude and latitude coordinates and translates them to a precise location on a map would trigger COPPA (FAQ 51).