SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

Skadden PRIVACY UPDATE

An Overview of Legislative, Regulatory and Technology Developments in the Privacy Sector

12.21.12

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact **Stuart D. Levi**, 212.735.2750, stuart.levi@skadden.com or your regular Skadden contact.

Four Times Square
New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

FTC Strengthens Online Child Privacy Regulations

After two years of proposals, discussions and comments, the Federal Trade Commission approved final amendments to the Children's Online Privacy Protection Rule (the "COPPA Rule" or "Rule")[1] on December 19, 2012. These amendments will require certain significant changes to the manner in which websites and online services interact with children.

Background to COPPA

As a general matter, the Rule, which implements the 1998 Children's Online Privacy Protection Act ("COPPA"),[2] prohibits the "operator" of a "website or online service directed to children" or any operator that has "actual knowledge that it is collecting personal information from a child" from collecting any "personal information" from a child under the age of 13 without (1) providing notice of what information is being collected and how that information is used and disclosed, and (2) obtaining "verifiable parental consent" for the collection, use or disclosure of information. COPPA also requires operators to maintain the confidentiality, security and integrity of personal information collected from children and prohibits operators from conditioning a child's participation in a game or other activity on the child's disclosure of more personal information than is reasonably necessary.

Since the Internet landscape has changed drastically since COPPA was enacted in 1998 — with the advent of social media, mobile browsing and apps, and the increased sophistication of targeted advertising — the FTC began considering changes to the COPPA Rule in 2010. The FTC initiated several rounds of public comments on draft amendments before releasing the final amended Rule.

Revisions to the Rule

As discussed below, the revised Rule significantly expands several key COPPA provisions: (1) it extends COPPA's application to websites or services that allow third-party plug-ins or advertising services to collect user information, and in some cases extends COPPA's reach to those third parties themselves; (2) it expands the definition of personal information to include photos and videos of children, geolocation data, and persistent identifiers such as IP address and device ID; (3) it strengthens data security and destruction provisions; and (4) it intensifies safe harbor oversight, among other things. The revised Rule goes into effect on July 1, 2013.

1. EXPANDED DEFINITION OF OPERATOR

COPPA applies to "operators" of websites or online services who collect or maintain personal information about their users or visitors, or operators on whose behalf personal

1 Children's Online Privacy Protection Rule (Dec. 19, 2012) (to be codified at 16 C.F.R. pt. 312), *available at* http://www.ftc.gov/os/2012/12/121219copparulefrn.pdf.
2 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 – 6506 (2012).

information is collected or maintained. The revised Rule modifies the definition of "operator" to clarify that personal information is collected or maintained on behalf of an operator when "(a) it is collected or maintained by an agent or service provider of the operator; or (b) the operator benefits by allowing another person to collect personal information directly from users of such website or online service."

This modification extends liability under COPPA to websites and online services that collect no information on their own but utilize plug-ins like Facebook's "like" button and Twitter's "tweet" button or third-party advertising services that collect personal information for their own use. Such sites and services will now be strictly liable for violations of COPPA's notice, consent and other regulations with respect to personal information collected by third parties. The rationale behind this expansion is that Web operators benefit from allowing third parties to collect information through their sites or services and are in the best position to know that their content is directed at children (triggering COPPA regulation) and to provide notice and obtain parental consent. This change reverses the FTC's previous policy of placing the burden of notice and consent entirely on the entity that collects information.

This change was widely criticized by online content providers and app developers, who argued that expanding the definition of "operator" in this way exceeded the FTC's authority under COPPA, pointing particularly to the data storage and management provisions of the act, which indicate that COPPA only was intended to apply to entities who have control over information collected. This argument was echoed by Commissioner Maureen K. Ohlhausen, who voted against adopting the amended Rule. It is Commissioner Ohlhausen's opinion that the application of COPPA to entities who do not have access to or control over information collected by a third party goes beyond the statutory definition of "operator," which only covers entities "on whose behalf such information is collected and maintained."

Industry members also argued that holding content providers strictly liable for data collection by third parties is overly burdensome for app developers and will stifle innovation in online content for children, particularly given the current online environment where content providers rarely have significant relationships or communication with third-party plug-in operators or ad networks. In response to further industry concern that the expanded definition would cover application marketplaces such as Apple's iTunes App Store and Google Play (formerly the Android Market), which provide access to child-directed content, the final Rule is drafted to specifically exclude such platforms by limiting COPPA's applicability to those entities that allow data collection "directly" from their users.

2. EXPANDED DEFINITION OF WEBSITE OR ONLINE SERVICE DIRECTED TO CHILDREN

COPPA originally applied only to operators of any "website or online service directed to children," which is defined to include any commercial website or online service or portion thereof that is "targeted to children." The revised Rule expands this definition to include a plug-in or advertising network operator when it has "actual knowledge" that it is collecting personal information through a child-directed website or service. The operator of a plug-in or ad network that falls within this definition is itself responsible for obtaining parental consent and protecting the confidentiality, security and integrity of personal information collected from children.

The actual knowledge standard represents a compromise between the FTC and technology industry. The August 2012 proposed Rule would have expanded COPPA's reach to any third-party service who "knows or has reason to know" that it collects information through a website or service directed to children. Industry members argued that this standard was vague and would impose a duty of inquiry on all third-party service providers to determine when a website or service could be considered "directed to children" under the Rule. The FTC recognizes that the actual knowledge standard is highly fact-specific but believes it will be met when, for example, a child-directed content provider directly communicates the child-directed nature of its content to the third-party service, or a representative of the online service recognizes the child-directed nature of the content.

It is not clear under the new Rule whether a website or online service operator will remain liable for data collection by third parties once those third parties are brought within COPPA's coverage by the new actual knowledge standard.

The factors to be considered in determining whether a website or online service is directed to children include its content, use of animated characters, child-oriented activities, use of child models, presence of celebrities who appeal to children, and advertising on the site that is directed at children. A potential issue with using such criteria is that many websites and social media platforms tailor the content and advertising they display to the particular user. Thus a website may appear to be directed at children when accessed by a child but not when accessed by an adult. Although targeting content and advertising at children is among the activities that COPPA seeks to prevent, it is possible that a site or service not directed at children could collect data without actual knowledge that a user is a child and accordingly tailor the child's user experience without running afoul of COPPA.

3. DISTINGUISHING BETWEEN CHILD AND ADULT USERS

Based on comments by online content providers that pointed out that many sites offer content that appeals to both children and adults, the revised Rule allows some online operators to differentiate among users, only requiring notice and parental consent for the collection of personal information for users who self-identify as being under the age of 13. The website and service providers who will be allowed to differentiate among users are those who fall under the definition of being "directed to children" based on the totality of the circumstances but do not target children under age 13 as their primary audience. Child-directed websites or services whose primary target audience is children under 13 must continue to assume all users are children and comply with COPPA regulations accordingly.

4. EXPANDED DEFINITION OF PERSONAL INFORMATION

Under COPPA, "personal information" means individually identifiable information including first and last names, address, email address, telephone number, Social Security number, or any other identifier that the FTC determines permits physical or online contacting of a specific individual. The revised Rule expands the definition of "personal information" to include screen or user names that function in the same manner as online contact information, photo, video and audio files that contain a child's image or voice, geolocation data and persistent identifiers that can be used to recognize a user over time and across different websites or online services.

a. Photo, Video and Audio Files

Photo, video and audio files were added to the definition of personal information both because they may be used to obtain other personal information about a child through metadata or facial and voice recognition technologies and because they are considered to be inherently personal. Under the Rule, any website, app or other online service that allows children to upload photos, videos or audio files depicting a child must comply with the notice and consent requirements of COPPA.

COPPA and the Rule generally contemplate the collection of personal information about a child from *that* child, however, under the expanded definition of personal information, it is possible that a child could upload a photo, video or audio file containing the image or voice of *another* child. The Rule does not attempt to distinguish between collection of personal information about a child from that child and collection of personal information about a child from a different child. It is entirely possible that a website or service that enables photo uploading could obtain parental consent for one child to use the site or service, but not for a friend who the child uploads a picture of. The website or service would then have collected information about a child, in the form of his or her photo, without parental notification or consent, in violation of COPPA. The Rule also requires that operators provide a reasonable means for parents to review the personal information collected from a child, which could be rather difficult under the above scenario if a website

or service collected photos of a child that were uploaded by another child and were in no way associated with the depicted child's name or other identifying information.

It also is not clear under the Rule whether the posting of a child's photo or video by an adult would be considered collection of personal information "from" that child. When a child's photo is uploaded to a website or service, that site or service has collected personal information about the child depicted, regardless of who provides it. Of course in the case that a parent uploads a photo, video or audio file depicting his or her own child, consent might be implied, but the situation is less clear when an adult shares information about a child who is not his or her own.

b. Geolocation Data

The FTC contends that the inclusion of geolocation data as personal information does not expand upon the existing definition, which considers any "physical address, including street name and name of city or town" to be personal information. This expansion will require parental notice and consent before any child uses a mobile app or website that offers geolocation services, as well as those that collect geolocation information for marketing or other purposes.

c. Persistent Identifiers

The inclusion of persistent identifiers as personal information prohibits websites and online services from collecting or allowing the collection of bits of personal information that are themselves insignificant, but when aggregated allow advertising networks and other service providers to compile a detailed profile of individual users. As a compromise between the FTC and industry, in order for a persistent identifier to be considered personal information, it must be used to collect information about a user or device both over time *and* across multiple sites or services. This allows individual site or service operators to use persistent identifiers to collect information within their site or service, which is important in conducting performance assessments and supporting intrasite preferences. Persistent identifiers will be considered personal information under the Rule when collected among unrelated sites or services or where the affiliate relationship is not clear to the user.

The final Rule also clearly exempts instances where an operator uses persistent identifiers for the sole purpose of providing support for internal operations. In addition to listing a number of activities that are considered to provide "support for internal operations," the final Rule creates a process by which operators may request FTC approval of additional services to be included within the definition. This exception for internal operations also will apply to the use of persistent identifiers by third-party data collectors who fall within the definition of "operator" for their own internal operations.

5. EXPANDED METHODS FOR OBTAINING PARENTAL CONSENT

Under COPPA, "verifiable parental consent" means any reasonable effort to ensure that a parent receives notice of and authorizes an operator's personal information collection, use and disclosure practices before that personal information is collected from their child. Additional acceptable methods of parental consent under the revised Rule include electronic scans of parents' signatures, video conferencing, government-issued identification (including a parent's driver's license or a segment of his or her Social Security number), and credit cards, debit cards or other electronic payment systems in connection with a monetary transaction.

The FTC considered but ultimately declined to adopt a platform method for parental notice and consent, whereby parents could receive notice and give their consent to information collection by all applications administered by a particular platform, gaming console, device manufacturer or other entity. The FTC did, however, note that nothing in the Rule prohibits operators from using a common consent mechanism as long as it complies with the Rule's basic notice and consent requirements. Operators also can propose common consent mechanisms through the voluntary commission approval process that is set forth in the final Rule.

6. TWO NEW EXCEPTIONS TO NOTICE AND CONSENT REQUIREMENTS

In addition to the existing exceptions to the notice and consent requirements set forth in COPPA and the prior Rule, the revised Rule adds two further exceptions.

First, the Rule allows websites or services that do not otherwise collect, use or disclose children's personal information to collect a parent's online contact information for the purpose of notifying the parent about the child's participation in the website or service.

Second, plug-ins, ad networks and other third-party operators who fall within the definition of "website or online service directed to children" (*i.e.*, those that meet the actual knowledge standard) may collect a persistent identifier (but no other personal information) from users who have a pre-existing relationship with the operator and have self-identified as being 13 or older. This exception applies only to users who affirmatively interact with the operator (*e.g.*, by clicking on a plug-in) and who have previously completed a registration with the operator. For example, this exception would allow an adult user with a Facebook account to click on a Facebook "like" icon on a website or in an app that is directed at children without triggering notice and consent requirements on the part of Facebook (assuming that Facebook were to meet the actual knowledge standard to be considered a "website or online service directed to children").

It is not clear that this exception applies to websites and services that do not collect information themselves but are liable as "operators" for data collection from their sites by third-party plug-ins or ad networks. Thus, in the example above, the website or app that is directed at children and contains the Facebook "like" plug-in might not fall within the exception. The exception also does not apply where a third-party operator collects other personal information along with the persistent identifier.

7. INCREASED DATA SECURITY REQUIREMENTS

The revised Rule requires operators to take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will do so. The final Rule is less stringent than an earlier proposed draft that would have required operators to "ensure" that third parties properly secured shared information.

The FTC also added a provision to the Rule regarding data retention and deletion. The provision requires that an operator retain children's personal information only as long as is reasonably necessary to fulfill the purpose for which the information was collected and then delete the information using reasonable measures to protect against unauthorized access to or use of the information.

8. INCREASED FTC OVERSIGHT OF SAFE HARBOR PROGRAMS

COPPA allows operators to satisfy the requirements of the act by following self-regulatory guidelines that are issued by representatives of the industry. This provision encourages industry groups to create and submit guidelines for complying with COPPA. If, after notice and comment, such guidelines are approved by the FTC as meeting the requirements of COPPA regulations, compliance with the guidelines will provide a safe harbor to operators. The FTC had approved four safe harbor programs by the time it released a first draft of proposed revisions to the COPPA Rule in 2011. The final Rules require safe harbor programs to submit more comprehensive self-regulatory guidelines, conduct annual reviews of each of their member's information practices and submit annual reports to the FTC containing an aggregated summary of the results of their member assessments.

Child Privacy as an FTC Priority

Protecting children's online privacy has been a top priority for the FTC. Just a week before publishing the revised Rule, the commission released a report revealing that mobile app developers have made little progress toward providing parents with sufficient information about how

mobile apps designed for children collect and share personal data and facilitate interaction with other services.[3] The report, which followed a similar one released in February 2012, found that many surveyed apps included interactive features or shared children's information with third parties without disclosing those practices to parents, noting that "most apps failed to provide *any* information about the data collected through the app, let alone the type of data collected, the purpose of the collection, and who would obtain access to the data." Only 20 percent of the apps surveyed by the FTC disclosed any information about privacy practices, while nearly 60 percent transmitted data to third parties, including device ID, geolocation and phone number.

The report recommends that the mobile app industry create and implement "best practices" for privacy protection and outlines additional steps that will be taken by the FTC staff to ensure that children's mobile apps properly handle personal identification information and comply with COPPA and FTC regulations.

The revised COPPA Rule and recent report serve as a reminder that the FTC is committed to protecting children's online privacy and that mobile app developers and other online service providers should take proactive measures to protect children's privacy and to disclose data collection activities.

California Lawsuit Serves as Important Reminder of State's Privacy Policy Law

On December 6, 2012, the California Attorney General filed suit against Delta Air Lines, alleging that the company's "Fly Delta" mobile app violates the California Online Privacy Protection Act (the "Act") by failing to "conspicuously post" a privacy policy.[4] This represents the first enforcement action filed under the California law since it was enacted in 2004, and serves as an important reminder to companies about California's privacy policy requirement, and specifically about its application to the ever-expanding world of mobile apps.

The Delta app offers customers a variety of services, such as the ability to check in, view reservations and pay for checked baggage. As part of the service, the app collects information including users' names, email addresses, frequent flyer numbers, geolocations and credit card numbers. Although Delta's website contains a privacy policy that complies with the Act, the stand-alone app does not. If found liable, Delta could face penalties of up to $2,500 per violation.

In October, Delta and other owners of top mobile apps were put on notice by the Attorney General that they were not in compliance with the state's online privacy law. At that time, Delta issued a statement describing its intent to comply with the law, but according to the complaint, Delta failed to do so within the 30-day period required.

The California Online Privacy Protection Act applies to all websites and online services — including mobile apps — that collect personally identifiable information from California residents. Personally identifiable information is defined as individually identifiable information about a consumer, including an individual's name, address, telephone number, email address, Social Security number or other identifying information. The law requires such sites and online services to "conspicuously post" and adhere to a privacy policy that must, among other things, identify the types of information collected and the categories of third parties with whom the information may be shared. The Act also requires websites and online services to disclose how consumers will be informed of material changes to the privacy policy.

The California Attorney General's action serves as an important reminder that any company that does business with California consumers (which likely covers most websites and online services) must have a conspicuous privacy policy. It also serves as a reminder that mobile apps are not outside the scope of the Act. Finally, the Attorney General's recent focus on mobile app developers may be an indicator that future enforcement actions will follow. In February 2012, the Attorney General reached an agreement with a number of companies in the mobile app market,

---

3 F.T.C. Staff Report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 10, 2012), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.

4 California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575 – 22579 (West 2012).

including Apple, Google, Microsoft, Amazon, Hewlett-Packard, Research In Motion, and later Facebook, to adopt a Joint Statement of Principles on enforcement of the state's privacy laws. In July 2012, the Attorney General created the new Privacy Enforcement and Protection Unit within the Department of Justice eCrime Unit, which is charged with enforcing the California Online Privacy Protection Act. The recent case against Delta Airlines represents another step in a more proactive approach by the California Attorney General's office.

Senate Judiciary Committee Considers Mobile Device Location Privacy Legislation

On December 13, 2012, the Senate Judiciary Committee approved legislation that would require mobile phone companies and application developers to obtain users' consent before collecting or sharing location data and would ban applications that secretly monitor a user's location (so-called "stalker" apps).[5] Although many mobile apps already obtain users' consent before using location data, the Location Privacy Protection Act would make the practice mandatory. With year-end quickly approaching, the bill is not likely to reach the Senate floor before the end of the session, but Sen. Al Franken, the bill's sponsor, is expected to continue to push the measure in 2013. It also is likely that the bill will undergo some modification in order to alleviate lingering bipartisan concern that the bill's restrictions could stifle innovation.

The act, if passed, would apply to any nongovernmental individual or entity who provides a service to an "electronic communications device," including phone manufacturers, application developers and wireless service providers. An "electronic communication device" is defined to include any device that enables electronic communication or geolocation service and is designed to be carried with a person, including a mobile phone, tablet, laptop or GPS-enabled vehicle. The bill does allow collection and use of location data without consent when necessary to locate a child or provide fire, medical, public safety or other emergency services, or when required by statute, regulation or judicial process.

The bill was introduced in 2011 amid increasing public concern over location data, prompted in part by a December 2010 *Wall Street Journal* investigation that revealed that, at that time, 47 of the top 101 smartphone apps disclosed users' location to third parties without consent.[6] While the Cable Act and the Communications Act prohibit cable and phone companies from disclosing customers' locations, similar disclosure by smartphone and app companies is currently permitted under what Sen. Franken describes as an "obscure section" of the Electronic Communications Privacy Act of 1986.

Both consumer groups and anti-stalking organizations support the bill, believing it will protect consumer privacy generally and will limit stalkers' and abusers' abilities to locate victims through their mobile devices. However, there is concern over how the bill would affect mobile device innovation, particularly for applications that rely on mapping and location data, and that might become too cumbersome to use if there is a consent requirement.

The act would apply only to the use of location data by nongovernmental entities. Tracking by governmental entities was addressed by the Supreme Court in January 2012 in *United States v. Jones*,[7] where the Court found warrantless GPS tracking to be a violation of the Fourth Amendment. On retrial in *Jones*, the government introduced tracking evidence based on cellphone tower location data. However, the district court avoided the question of whether warrantless collection of non-GPS location data is similarly unconstitutional, relying instead on the police officers' reasonable, good-faith belief that the tracking was lawful.[8]

---

5 Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011).
6 *Your Apps Are Watching You*, The Wall Street Journal, Dec. 17, 2010.
7 132 S. Ct. 945 (2012).
8 *United States v. Jones*, No. 1:05-cr-00386 (D.D.C. Dec. 14, 2012).