Extracted from *Law360*:

No Cookie for You: How COPPA Will Affect Your Company

By Dominique Shelton and Claire Lucy Readhead

Law360, New York (August 05, 2013, 12:50 PM ET) -- 2013 is the year of "big data" and the collection of information through behavioral tracking and mobile apps for consumer behavior analysis. The collection and analysis of consumers' personal information and behavior, amassed in big data, are necessary for companies to remain competitive in the contemporary marketplace of targeted advertising, personalized offerings and customized services. The amalgamation and analysis of this personal data raises significant privacy concerns and may result in costly litigation and/or penalties for companies if not handled with care. This is evidenced by over 200 privacy class actions that are pending around the country and the Seventh Circuit's recent class certification consisting of 10 million class members in a consumer privacy lawsuit against ComScore.

Companies are particularly vulnerable to privacy litigation and regulatory enforcement regarding the collection of behavioral data from children. With the advent of mobile marketing, and children's rapidly increasing use of mobile apps, both the Federal Trade Commission and plaintiffs' attorneys have targeted the issue of children's privacy in light of developing technology.

In response to class action litigation concerning the collection of personal information from children on websites and mobile devices and consumer concerns, the FTC amended the Children's Online Privacy Protection Act to clarify the extension of the rule to new technologies (like mobile apps) and strengthen its protection of children's privacy. The amended COPPA rule, effectuated July 1, 2013, expands the definition of personal information to cover behavioral tracking, clarifies the definition of geolocation and adds an exception to the rule prohibiting use of persistent identifiers to track children, where the website needs this information for internal operations.

The amended rule impacts many companies, especially those with websites and apps directed to children, because companies often use persistent identifiers and geolocation to develop behavioral profiles for big data analysis and marketing purposes. The use of big data to track behavior is becoming increasingly common; however, such techniques may come at a heavy price where operators run afoul of federal and state privacy regulations.

Understanding these amended COPPA rules in the context of behavioral data is crucial given the fact that regulatory statutory fines are $16,000 per violation, private statutory damages are $2,500 per violation. These statutory claims can add up where there are alleged millions of tracking violations. For example, outside of the COPPA context, ComScore was faced with a behavioral tracking claim amounting to over $1 billion in exposure. Also, a behavioral tracking class action was filed against Lowes alleging $400 million in statutory damages.

With regard to children's apps, in February 2013, the Path social networking site paid $800,000 to settle the FTC charges that it allegedly collected children's personal information without the knowledge or consent of his or her parent and is defending three class actions regarding same. Given the hefty penalties associate with COPPA violations, ongoing litigation concerning children's digital privacy will serve as useful guidance to see how courts and the FTC will implement and enforce the amended COPPA rule. In addition, the FTC's clarification of its rule on geolocation has a retroactive effect, therefore developments in COPPA litigation may illustrate how courts and the FTC will interpret and implement the amended rule.

The Effect of the Amended COPPA Rule

The amended rule expands the definition of personal information to include: (1) persistent identifiers (even when they are not combined with additional identifying information like a name or address);[1] (2) photos, videos, or audio recordings of children; and (3) screen or user name; and (4) geolocation.[2]

Further, the FTC explains that adding geolocation as a standalone category of personal information, is merely a clarification of the old rule. The old rule included geolocation in its definition of personal information, therefore companies must obtain parental consent regardless of when it collected geolocation data.

The amended rule also creates an exception for child directed sites and third party plug-ins to collect behavioral data by using persistent identifiers to track children where the information is used for the support of internal operations. The FTC defines internal operations as those things necessary for an online service's support such as to "(a) maintain or analyze the functioning of the website or online service; (b) perform network communications; (c) authenticate users of, or personalize the content on, the Web site or online service; (d) serve contextual advertising on the Web site or online service or cap the frequency of advertising; (e) protect the security or integrity of the user, Web site, or online service; (f) ensure legal or regulatory compliance; or (g) fulfill a request of a child." [3] The term "internal operations" does not include information used to contact an individual or behavioral advertising.

The new COPPA rules now render child-directed websites and online services strictly liable for plugs-ins (e.g., Facebook, Twitter and Instagram) that track children on their sites. It is common for website to have plug-ins like "follow us on Twitter" with a plug-in to the Twitter logo that hyperlinks to the platform. These plug-ins often use cookies, or other tracking technologies to track referrals from host websites. Now, child-directed host websites will be strictly liable if the plug-ins track children. Further, the social networks will be liable if they have actual knowledge that they are plugged into (and therefore tracking from) child-directed websites.[4]

What should companies do if they have already invested in "big data" management platforms or partner relationships but their databases include behavioral information gathered before and after the July 1, 2013, effective date of the COPPA rules. Will the new COPPA rules have retroactive effect? According to the FTC's answers of frequently asked questions on its website, the answer is yes, in some respects, but the precise scope of retroactivity or the extent exceptions might apply remains unclear.[5]

The answers may emerge in the pending putative class actions and future regulatory actions in the months ahead. Below are a few cases to watch that involve allegations of behavioral tracking of children through mobile apps.

Children's Privacy and Behavioral Tracking

Viacom's Tracking Cookies

In December 2012, plaintiffs filed six separate putative class actions in different jurisdictions.[6] The alleged classes consisting of minor children brought suit against Viacom Inc. and Google Inc. for allegedly tracking children's Internet communications and video viewing habits. Plaintiffs allege Viacom and Google impermissibly collected children's personal information including birthdates and unique device identifiers (the numerical values assigned to their mobile devices), without parental consent.

In June 2013, Viacom and Google successfully moved to have the six class actions transferred to New Jersey. As behavioral tracking and persistent identifiers are at issue in this pending litigation, it should be watched to determine how collection of geolocation and behavioral data is treated in the context of the recently amended COPPA rule.

Path Litigation

Companies should also monitor the ongoing series of class actions against Path Inc. for guidance on compliance with the amended COPPA rule as it relates to the issue of using unique identifiers that may track children.[7] In the Path litigation, plaintiffs allege Path impermissibly collected children's personal information without parental consent. Plaintiffs also assert Path illegally monitored children's online social network interactions by using geotagging with digital contact to implement tracking cookies. Path takes the position that it is a general audience online service that does not target children.

These class actions are still in litigation and remained unresolved. However, Path agreed to settle with the FTC for charges of collecting personal information without user's knowledge or consent. According to the

settlement, Path will pay $800,000 to settle the charges that it illegally collected personal information form children without their parents' consent.

CDD Complaints

Also of interest are the recent FTC complaints brought by the Center for Digital Democracy, urging the FTC to investigate and bring action against Nickelodeon for its Mobile SpongeBob Dinner Dash game app. The CDD claimed that the SpongeBob app impermissibly collected child's unique device identifier, a string of numbers that can be used to uniquely identify a child's mobile device," without parental consent and in violation of COPPA.

Although at the time persistent identifiers were not included in COPPA's definition of personal information, Nickelodeon temporarily pulled the app to investigate the CDD's complaint. That same year, the CDD also brought a similar request for investigation against the Mobbles Corporation for its collection of children's personal information through its virtual pet game app. The CDD explicitly complained that the app collected information on children's precise physical location without verifiable parental consent. In response, Mobbles immediately pulled the app for review.

While those pending complaints are concluded, companies should look to the FTC's public complaints to obtain guidance regarding how the new COPPA rules will be applied in the context of big data analytics.

Conclusion

With the rapidly increasing number of children who use mobile apps, companies must be aware of and understand the FTC's expansion of COPPA's definition of personal information to include persistent identifiers, the retroactive effect of the clarification of geolocation and the scope of any applicable exception for internal operations.

Recommendations for Best Practices

- If you are a child-directed website, understand you are strictly liable for plug-ins that track users on your website. Consider entering into agreements with the plug-ins to prevent the use of persistent identifiers for tracking or obtaining confirmation that this tracking information will be used for internal operations, only.

- If your website is "plugged-in" to others, consider disable tracking if you become aware that you are collecting persistent identifiers from children under the age of 13.

- Find out whether your company's mobile app uses persistent identifiers or other tracking technologies. If your app is directed to children, obtain parental consent before gathering.

- If you have a data management platform that contains children's information that was legally gathered before July 1, 2013, do not add new data that is prohibited to it after July 1, 2013.

- Carefully review your information practices and online privacy policy. Ensure you are not collect information, covered under the amended COPPA rule, from children under the age of 13.

- If you want to use behavioral data for marketing, be sure to segregate "big data" databases between pre-July 1, 2013 and post July 1, 2013.

- If your website is directed to children under the age of 13, ensure your privacy policy discloses the following:

    - The name, address, telephone number and email address of all operators collecting or maintaining personal information through the site or service;

    - A description of what information the operator collects from children;

    - Whether the operator enables children to make their personal information publicly available;

    - How the operator uses information collected from children;

    - The operator's disclosure practices for information collected from children; and

    - That a parent can review and delete child's personal information and refuse further collection and use.

    - Note: Do not include promotional materials in privacy policy.

- Retain child's personal information for only as long it is necessary to fulfill the purpose for which it was collected.

- Take reasonable steps to protect children's personal information.

Dominique Shelton is a partner and Claire Lucy Readhead is an associate in Alston & Bird's litigation and trial practice group in Los Angeles.

[1] A persistent identifier is one in which can be used to recognize a user over time and across different websites or online services.

[2] These types of information add to what was previously considered PI, including: (1) first name; (2) last name; (3) home or other physical address; (4) online contact information; (5) telephone number; (6) social security number; and (7) geolocation sufficient to identify the street name and name of city or town.

[3] 16 C.F.R. § 312.5(c)

[4] 78 Fed. Reg. 3975-3979 (Jan 17, 2013).

[5] Complying with COPPA: Frequently Asked Questions, Section A GENERAL QUESTIONS ABOUT THE COPPA RULE, Question 4 located at http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#COPPA

[6] See N.J. v. Viacom Inc.; K.T. v. Viacom Inc. & Google Inc.; T.M. v. Viacom Inc.; CAF & CTF v. Viacom Inc. & Google Inc.; L.G. v. Google Inc. & Viacom Inc.; Stephanie Fryar v. Viacom Inc.

[7] See Hernandez v. Path Inc.; Operman et al. v. Path Inc.; United States of America v. Path Inc.; Sterk v. Path Inc..