

FTC Announces Investigations of Kids App Providers and California's AG Sues Delta over Fly Delta App's Privacy Practices

Two recent developments should have all app providers reviewing their privacy practices and policies. On Monday, December 10, the Federal Trade Commission released its latest report on privacy disclosures and kids apps. Finding industry to have made “little or no progress in improving its disclosures,” the FTC announced that it “is launching multiple non-public investigations” into mobile app providers. And in California last Thursday, December 6, California's Attorney General followed up on the notices she provided to app providers in October and sued Delta Air Lines for failing to post a privacy policy in its *Fly Delta* app. In both developments, the government agencies chastised companies for failing to provide app users with sufficient, accurate information regarding what data is being collected and shared by apps. The FTC in its Kids App Report also expressed significant concerns with the aggregation of data by a handful of companies.

The FTC Report

The FTC recent Report, “*Mobile Apps for Kids: Disclosures Still Not Making the Grade*,” is the FTC's second survey of privacy disclosures and practices of mobile apps aimed at kids. The first was released about a year ago. Entitled, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, the earlier report concluded that little information was available then to parents about the privacy practices and interactive features of the mobile apps surveyed.

In its latest report, the FTC concludes that parents still are not given basic information about the privacy practices and interactive features of mobile apps aimed at kids. According to the agency, many apps surveyed do not disclose that they collect and share personal information regarding users or the devices on which their apps are loaded or, if they have disclosures, their disclosures are misleading. This reportedly includes failing to inform parents that the apps share device IDs or geolocation data.

The FTC's latest report was also critical of the perceived lack of notice to parents of the existence of advertising in apps, the ability of users to make in-app purchases and the ability to link to social media, like Facebook, from within apps. The FTC went so far as to include screenshots of a painting app to illustrate its point. One was of the app promotion page, which touted the app as “The BEST painting program for kids!” Another was from within the app, which shows a child-like drawing and an ad from on an-line dating site to “See **1000+** Singles.” The screenshot of the app's promotion page showed no ads.

Particular emphasis also was placed on the transmission and sharing of device IDs by apps and the concentration of data in the hands of a few shared data recipients. Noting that 59% of the apps transmitted some device ID to an app developer or third party, the FTC stated that “[c]oncerns about the creation of detailed profiles based on device IDs become especially important where, as staff found, a small number of companies (like ad network and analytics providers) collect device IDs and other user information through a vast network of mobile apps.” Of the 400 apps the FTC observed, 100 reportedly sent data to one third party, 80 to another, and 66 to yet another.

As for next steps, the FTC announced that it has launched “a number of investigations to address the gaps between company practices and disclosures.” Specifically, the Agency will investigate whether these gaps violate the Children's Online Privacy Protection Act or constitute unfair or deceptive trade practices. It also intends to develop education programs and conduct future surveys.

California AG's Action

Following up on the notice letters her office sent some 100 app providers in late October (See Ropes & Gray's November 5th [Alert](#)), California Attorney General Kamala Harris sued Delta Air Lines on December 6 under California's Unfair Trade Practices Act for the alleged failure of its Fly Delta app to comply with the California Online Privacy Protection Act ("CalOPPA"). The complaint also alleges a separate statutory violation of CalOPPA for the failure of Delta's Fly Delta app to comply with the terms of the privacy policy located on the Delta website. The Attorney General alleges the latter claim does not require her to give 30 days' notice before bringing an action. The Attorney General seeks \$2,500 for each violation of the California Unfair Trade Practices Act, alleging that the Fly Delta app has been downloaded by consumers millions of times.

Section 2275 of CalOPPA generally requires the "operator of a commercial website or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial website or online service" to "conspicuously post" its privacy policy on its website or make it available, "[i]n the case of an operator of an online service, [by] any other reasonably accessible means of making the privacy policy available for consumers of the online service." A violation of this requirement occurs if the operator fails to correct a deficiency within 30 days of notice, and is the provision Attorney General Harris relied upon in sending her notice to Delta.

Upon receiving the notice, Delta allegedly issued a press release stating that they "intend to provide the requested information." However, by the date the complaint was filed, Delta apparently had not updated its app to conspicuously post a privacy policy.

The Attorney General's office did review the privacy policy on Delta's website. It allegedly found gaps between what that policy said and the practices of the app. The Fly Delta app allegedly collects geolocation data and photos submitted by users. The Delta website does not, and the privacy policy on the Delta website does not mention the app nor does it mention that the app collects geolocation data and photos. This gap appears to be the foundation for the separate claimed CalOPPA violation, for which the Attorney General alleges no pre-suit notice is required.

The California Attorney General's complaint demonstrates the hard spot companies may find themselves in if they neglect to include privacy policies within apps – as both the FTC and California Attorney General are pushing for – and if their privacy policies do not keep up with the myriad ways that their products and business lines collect and share data on consumers. That is, generic privacy policies and practices may not provide a sufficient shield in the face of challenges from government officials who are increasingly looking beyond whether a company simply has a privacy policy to examining what it is companies are actually doing with consumer data.

For more information regarding strategies for responding to FTC or Attorney General investigations or other data handling and security concerns you may have, please contact a member of our leading [privacy and data security](#) team, including [Jim DeGraw](#), [David McIntosh](#), [Doug Meal](#), and [Mark Szpak](#).