wiley

NEWSLETTER

FTC Sanctions Snapchat for Falsely Claiming That Photos Would Disappear

June 2014

In a reminder of the importance of doing what your privacy policy says you are doing, the Federal Trade Commission (FTC) announced in May that the developer of the highly popular Snapchat mobile message app has agreed to settle charges that it had misrepresented the "disappearing" nature of messages sent through the service.

Alleged App Failings

The Snapchat app allows users to send photos and videos that would, Snapchat touted in its promotions, "disappear forever" after expiration of a time period chosen by the sender. However, the FTC alleged that, in fact, there were several "simple ways" in which the "snaps" would not "disappear" at all. For example, the FTC noted that widely-available third-party apps would enable users to view and save snaps indefinitely. And the app stored video snaps unencrypted in a place readily accessible on a user's device from a connected computer terminal. Indeed, the FTC said that the "disappear" functionality depended upon use of the app itself, and a third-party viewing and saving apps circumvented that feature.

The FTC also cited other ways in which the app did not live up to the claims made by Snapchat. For example, although Snapchat claimed that the sender would be notified if the recipient took a screenshot of a snap, recipients using certain older versions of iOS could easily avoid this detection, and no notice would be sent.

Other charges reflect issues that the FTC has cited frequently regarding mobile apps. First, the agency's complaint charged that Snapchat transmitted location information via its Android app despite asserting in its privacy policy that it did not do so. Second, the FTC charged that for a period of time the app collected iOS users' contact information from the devices without providing notice or an opportunity for users to consent or deny that collection. Third, the FTC charged that Snapchat did not secure the "Find Friends" feature of its app, despite the company's claims about taking reasonable security steps, by failing to verify users' phone numbers during registration. This led some users to send their personal "snaps" to complete strangers who had registered phone numbers that did not belong to them.

Enforcement Implications

As is the FTC's standard practice, the proposed consent decree will require Snapchat to cease its misrepresentations. Going forward, the company also has agreed to put in place a comprehensive privacy program subject to independent monitoring for 20 years—a period of time longer than text messaging has been available. The program must address privacy risks related to the development and management of new and existing products and services for consumers, and protect the privacy and confidentiality of information collected or accessed through Snapchat.

So what does this mean? First, the case highlights how important it is for app developers to review the accuracy of their marketing representations, with particular attention to how the app will function on both the iOS and Android platforms, and on different versions of those platforms.

Second, the case serves as a reminder that app developers should not write apps that routinely collect users' contact information or geolocation without providing notice to the users and an opportunity for them to consent or block collection of that information. Here, the FTC was able to identify an alleged misrepresentation, thus enabling it to proceed on a "deceptive" trade practice theory.

Third, the FTC takes mobile app security seriously. In this case, the app was written in such a way as to allow individuals to create Snapchat accounts with phone numbers belonging to other persons. As a result, users sent snaps to total strangers, thinking they were being sent to their friends. This flaw existed from October 2011 to December 2012 before being corrected.