Snapchat Captured in FTC Enforcement

May 11, 2014

On May 8, 2014, the FTC announced a settlement with Snapchat resolving allegations that the popular mobile messaging app deceived consumers over the disappearing nature of users "snaps" and made false and misleading representations concerning its privacy and information security practices. The FTC took issue with several of Snapchat's practices and representations:

- ***Disappearing "Snaps"*** – Snapchat represents to users that their snaps (*i.e.,* photos and videos) will "disappear forever" after the user-set time period expires, thereby ensuring users' privacy and safeguarding against data collection. According to the FTC's complaint, however, recipients could circumvent the settings to save or access the snaps in a number of ways. For example, recipients could open Snapchat messages in third-party apps, take a screen shot of the snaps on an iPhone, or access videos by connecting their mobile device to a computer and retrieving the files through the device directory. The complaint alleges that these types of workarounds were highly publicized.

- ***Misrepresenting Data Collection Practices*** – Snapchat's privacy policy represented to users that the app did not access or track users' geolocation information. The FTC complaint asserts that in October 2012, Snapchat integrated an analytics tracking service in the Android system, which transmitted Wi-Fi based and cell-based location information from users' mobile devices. Snapchat continued representing in the privacy policy that it did not collect or use geolocation information until February 2013. In addition, the app allows users to "Find Friends" by entering their mobile number or by accessing the Find Friends feature in the apps menu options. The privacy policy implied that the user's mobile phone number was the only information Snapchat collected to find the user's friends. The FTC contends, however, that when the user chose to Find Friends, Snapchat also collected the names and phone numbers of all the contacts in users' address books.

- ***Security Design Flaws***: The FTC complaint alleges that Snapchat failed to securely design its Find Friends feature by failing to verify the phone number of the user upon registration. In such case, an individual could create an account using a phone number belonging to another consumer. The FTC contends that Snapchat received a number of complaints that users' snaps were being sent to strangers who had registered with friends' numbers, or that their phone number had been used to send inappropriate or offensive snaps. In addition, Snapchat represents in its privacy policy that it takes "reasonable steps" or "reasonable measures" to protect users information. The FTC asserts, however, that Snapchat failed to implement any restrictions on serial and automated account creation, which allowed attackers to create multiple accounts and send millions of Find Friends requests using randomly generated phone numbers. According to the complaint, the attackers were able to compile a database of 4.6 million Snapchat usernames and associated mobile phone numbers.

The FTC's proposed consent order prohibits Snapchat from misrepresenting: (1) the extent to which

a message is deleted after being viewed by the recipient; (2) the extent to which the company or its products or services are capable of detecting or notifying the sender when a recipient has captured a screenshot of, or otherwise saved, a message; (3) the categories of covered information collected; or (4) the steps taken to protect against misuse or unauthorized disclosure of covered information.

Although the FTC's order does not include any monetary remedy, Snapchat must comply with a 20-year FTC administrative order. This means that if the company violates a term of its settlement agreement with the FTC, it can be liable for a civil penalty of up to $16,000 for each violation, which the FTC can construe as each day of non-compliance. The settlement is a continued reminder that the FTC remains focused on protecting the privacy of consumers and will closely scrutinize companies' practices as they relate to the handling and security of consumers' personal information.