FTC Says “Stalking” Apps Violate COPPA and the FTC Act

Article By
Sheila A. Millar
Tracy P. Marshall
Keller and Heckman LLP
Telecom Business Alert

- Communications, Media & Internet
- Consumer Protection
- All Federal

Wednesday, October 30, 2019

You know that movie where a person thinks they’ve barricaded themselves in their house against a stalker, only to grasp the awful realization that the threat is “coming from inside the house”? Unbeknownst to you, that threat may, in fact, be coming from your smartphone, according to a complaint by the Federal Trade Commission (FTC). The FTC recently took action against developers of three mobile apps that were, according to the Complaint, “designed to run surreptitiously in the background” and “uniquely suited to illegal and dangerous uses.” The Complaint alleged violations of the FTC Act and Children’s Online Privacy Protection Act (COPPA).

The FTC Complaint

Marketed as tools for parents to monitor their children and for employers to monitor employees, three mobile apps operated by Retina-X Studios – MobileSpy, TeenShield, and PhoneSheriff – tracked location and mobile device use, but without a user’s knowledge or consent. The apps collected text messages, call history GPS locations, photos, contact lists, browser history, and other information. According to the FTC, the information collected was not properly secured, despite the company’s promises to the contrary. Even after hackers penetrated the company’s cloud storage account twice in a one-year period, leading to the exposure of personal information, the company’s privacy policies insisted that “Your private information is safe with us.” The company also allegedly outsourced much of its product development and maintenance to third parties without sufficient oversight, such as conducting
security testing on the apps.

Retina-X’s privacy protections were also allegedly lacking, and, in some instances, allowed users to flout protections designed to alert them about tracking. Default settings in the apps used an icon to inform users that they were being monitored, but the company provided purchasers with instructions on how to turn this feature off, leaving device users who installed the app in the dark about the fact that they were being tracked. The FTC also claimed the company took no steps to validate that the apps were only used to monitor children and employees. Another serious concern prompting the FTC to act was the possibility that domestic abusers and other stalkers could access a device where the app was installed and emotionally and physically abuse an unwitting victim.

The Order

The proposed consent order requires Retina-X and its principal to delete all data collected from the “stalking apps,” prohibits them from misrepresenting their privacy and security practices, and bans them from selling, promoting, or distributing monitoring apps or services that require circumventing the manufacturer’s security protections. The homepage of any website advertising the apps must clearly and conspicuously state that the apps may only be used for legitimate and lawful purposes by authorized users, and the company must obtain express written confirmation from purchasers that they will only use the app for legitimate and lawful purposes, such as a parent monitoring a child, an employer monitoring an employee who has consented, or an adult monitoring another adult who has consented.

Similar to other FTC Orders, Retina-X is required to implement and maintain a comprehensive information security program and obtain third-party assessments of its security program every two years by an assessor the FTC may approve. The company must designate a senior corporate manager to administer the security program and certify compliance annually.

While these security obligations are now standard in FTC consent agreements, this is the first time the FTC has brought a case against monitoring apps. It comes on the heels of the FTC’s COPPA Rule workshop that explored possible updates to the COPPA Rule to address changes in technology. This action establishes that COPPA and Section 5 of the FTC Act give the FTC authority to take action against app developers that circumvent security measures. The FTC has made it clear that safeguarding consumers from potential emotional or physical threats made possible through the surreptitious installation of a stalking app is just as important as protecting them from risks of identity theft and similar harms associated with privacy and security failures.

© 2020 Keller and Heckman LLP