GIBSON DUNN

November 1, 2019

FTC BRINGS FIRST CASE AGAINST TRACKING APPS

To Our Clients and Friends:

On October 22, 2019, the Federal Trade Commission announced the first-of-its-kind enforcement action and settlement against the developer and marketer of three tracking applications, Retina-X Studios, LLC and James N. Johns, Jr. In this unprecedented action, the FTC alleged that Retina-X and Johns failed to take basic steps to protect sensitive personal data collected from their so-called "stalking" mobile applications, in violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a) and the Children's Online Privacy Protection Act ("COPPA") Rule, 16 C.F.R. § 12. The FTC's action may presage further enforcement activity against firms and individuals providing technology that can enable privacy abuses, especially when children are involved.

Background

The FTC alleged that Retina-X and Johns developed and marketed three mobile apps—MobileSpy, PhoneSheriff, and TeenShield—that allowed purchasers to monitor third parties without their knowledge or consent. In announcing the settlement, Andrew Smith, the Director of FTC's Bureau of Consumer Protection, recognized that "although there may be legitimate reasons to track a phone, these apps were designed to run surreptitiously in the background and are uniquely suited to illegal and dangerous uses."[1]

The complaint alleged that the three apps collected sensitive personal information and did not take adequate steps to secure the information, in violation of the FTC's prohibition against unfair and deceptive practices and COPPA. Under Section 5 of the FTC Act, a practice is unfair if it causes or is likely to cause substantial injury to consumers, cannot be reasonably avoided by consumers, and is not outweighed by countervailing benefits to consumers. The FTC's COPPA Rule imposes certain data collection and disclosure obligations on operators of websites or online services that collect, use, or disclose personal information from children under 13. As alleged, MobileSpy, marketed as a product to monitor children or employees, was launched in 2007 and sold more than 5,700 licenses. PhoneSheriff, marketed as a product to monitor children, was launched in 2011 and sold more than 5,000 licenses. TeenShield, marketed as a product to monitor children, was launched in 2015 and sold more than 5,000 licenses. As part of the registration process, TeenShield required the purchaser to input the date of birth of the person being monitored. Between February 2016 and October 2017, TeenShield collected about 950 dates of birth, a third of which were for children under the age of 13. Once installed, the apps collected and stored, among other data: text messages, call history, keys pressed, GPS locations, photos, contact lists, browser history, music files, notes, calendar entries, other apps installed, usage summaries, and email history. The Premium version of MobileSpy allowed consumers to access the monitored device in real time. PhoneSheriff was able to store screenshots of Snapchat activity.

To install the apps, purchasers were often required to "jailbreak" or "root" the mobile device by bypassing device manufacturer restrictions, which the FTC alleged unknowingly exposed the device to security vulnerabilities and likely invalidated manufacturer warranties. Further, the FTC alleged that the apps provided purchasers instructions about how to remove the app's icon from appearing on the mobile device screen, so that device users would remain unware that they were being monitored. The FTC pointed to these features—the use of jailbreaking and surreptitious monitoring—in concluding that the three apps in question were more likely used by stalkers and abusers to collect victims' physical movements and online activities, and then used to "perpetuate stalking and abusive behaviors, which cause mental and emotional abuse, financial and social harm, and physical harm including death."[2]

Finally, the FTC alleged that on two occasions, hackers were able to access data from the Retina-X servers that had been collected from the monitoring apps. All three apps have not been available for purchase since 2018, but the websites remain accessible.

Settlement Terms

Retina-X and Johns did not admit or deny any allegations in the FTC's complaint except for the language in the Settlement Order. The proposed settlement will be subject to public comment for 30 days after publication in the Federal Register and the FTC will then decide whether to make the proposed consent order final.

Under the proposed settlement, Retina-X and Johns agreed to refrain from selling monitoring apps that require circumvention of mobile device manufacturer's security protections. Retina-X and Johns are required to obtain written confirmation from purchasers that their products will be used only for legitimate purposes. Any monitoring products must be used only by parents monitoring their children, employers monitoring consenting employees, or adults monitoring other consenting adults. Further, the app icon with the name of the app must be visible on the device's screen unless the app is installed by a parent on their minor child's device.

The proposed settlement also requires Retina-X and Johns to destroy all personal information collected from the three monitoring apps every 120 days, and to implement and maintain a comprehensive information security program to protect any personal information collected in the future. Retina-X and Johns must retain a senior corporate manager to oversee the information security program and certify compliance with the order every year. Retina-X and Johns must also obtain third-party assessments of their security program every two years for twenty years.

What To Expect

The FTC's action against Retina-X and Johns may portend further enforcement and legislative action around technologies that can be used to enable alleged domestic violence, cyberstalking, and COPPA violations.

Following the announcement of the proposed settlement, the FTC released a warning to consumers about stalking apps[3] and cautioned other companies that sell monitoring products to ensure that their products are "used only for lawful purposes." The FTC announced that companies cannot "require the

circumvention of built-in operating system or device security protections and then claim ignorance about how [the product] is used." When working with third-party service providers, the FTC instructed companies to "spell out [] data security expectations in [] contracts and build in monitoring mechanisms to make sure [the third parties] are following through."[4]

Beyond the FTC, other civil and criminal authorities likely will consider further intervention to address growing concern about cyberstalking and other forms of technology-enabled domestic violence. In most states and at the federal level, cyberstalking is a crime. Under the federal statute, cyberstalking includes any course of conduct taken by the perpetrator on the Internet that places the victim in reasonable fear of death or serious bodily injury, or causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to the victim or the victim's immediate family.[5] Other potentially applicable statutes include the Computer Fraud Abuse Act of 1986[6], which makes it a criminal offence to access a computer, tablet, or smartphone without authorization; the Electronic Communications Privacy Act of 1986[7], which prohibits interception and disclosure of wire, oral, and electronic communications; and the Violence Against Women Reauthorization Act of 2013[8], which makes cyberstalking part of the federal interstate stalking statute.

Finally, privacy advocates and legislators have proposed new legislation imposing criminal and civil penalties specifically on cyberstalking apps. Since 2011, several United States Senators have called on key federal agencies to investigate stalking apps, and since 2015, various legislators have introduced federal legislation that would prevent the development, use, and sale of tracking apps.[9]

We expect there to continue to be various legislative proposals put forward, though, given the complexity and sensitivity of the issue, no particular proposal has yet garnered broad bipartisan support. We will continue to monitor developments in this area.

---

[1] Press Release, Federal Trade Commission, FTC Brings First Case Against Developers of "Stalking" Apps" (Oct. 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps.

[2] In the Matter of Retina-X Studios, LLC. Complaint, https://www.ftc.gov/system/files/documents/cases/172_3118_-_retina-x_studios_complaint_updated.pdf.

[3] Lisa Weintraub Schifferle, *Stalking apps: Retina-X settles charges*, FTC Consumer Information (Oct. 22, 2019), https://www.consumer.ftc.gov/blog/2019/10/stalking-apps-retina-x-settles-charges.

[4] Lesley Fair, *FTC takes action against stalking apps*, FTC Business Blog (Oct. 22, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/10/ftc-takes-action-against-stalking-apps.

[5] 18 U.S.C. § 2261A (2015).

[6] 18 U.S.C. § 1030.

[7] 18 U.S.C. § 2511.

[8] 34 U.S.C. § 12441.

[9] Location Privacy Protection Act of 2015, S. 2270, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/senate-bill/2270/cosponsors.

The following Gibson Dunn lawyers prepared this client update: Alexander Southwell, Matthew Benjamin and Praatika Prasad.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work or any of the following leaders and members of the firm's Privacy, Cybersecurity and Consumer Protection practice group:

United States

Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
M. Sean Royall - Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Olivia Adendorff - Dallas (+1 214-698-3159, oadendorff@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Europe

Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Jean-Philippe Robé - Paris (+33 (0)1 56 43 13 00, jrobe@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)

Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)

Asia
Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)