MORRISON | FOERSTER

Morrison & Foerster Client Alert

December 6, 2013

FTC Expands Reach on Conspicuousness of Privacy Disclosures in Settlement with Android Flashlight App

By D. Reed Freeman, Jr. and Adam J. Fleisher

An FTC settlement with a mobile app over its privacy disclosures alleged to be deceptive may seem to be run-of-the-mill. After all, the FTC has been settling cases for years with companies whose data collection and use practices are allegedly not consistent with the representations those companies make in their privacy policies.

But the FTC's Complaint and Order with Goldenshores Technologies ("Goldenshores"), announced on December 5th, is a particularly noteworthy Section 5 case because the FTC's theory is that the company's alleged violation of Section 5 resulted not out of an affirmative representation regarding its app alleged to have been deceptive, but from an alleged *material omission*, and from an allegation that whatever disclosures there were *did not rise to the required level of prominence because they were in the privacy policy and EULA only*.

These types of allegations and policy determinations have heretofore been limited to spyware, and have crept into online behavioral advertising, but have generally not been part of FTC enforcement actions in other contexts. **This case represents the FTC's signal to industry that material facts, especially those involving sensitive data, and especially where the facts involve collection, use, or disclosure of data that may surprise ordinary users because it is out of context of the use of the service, must be disclosed not only in a privacy policy, but also outside the privacy policy, clearly and conspicuously, prior to collection of the data.**

THE APP'S COLLECTION AND USE OF "SENSITIVE DATA"

Goldenshores is the developer of the immensely popular "Brightest Flashlight Free" flashlight app (the "app") for Android devices. The **FTC Complaint** explains that the app can be downloaded from the Google Play application store, amongst other places. The gravamen of the FTC's Complaint stems from the allegation that while the app is operating as a flashlight (using the phone's screen and LED

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
James R. McGuire (415) 268-7013
Daniel F. Muto (858) 720-7959
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Peter McLaughlin (212) 336-4290
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
L. Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Ann Bevitt 44 20 7920 4041
Anthony Nagle 44 20 7920 4029
Caroline Stakim 44 20 7920 4055
David Varney 44 20 7920 4058

ASIA

Beijing
Gabriel Bloch 86 10 5909 3367
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

flash for the camera) it is also collecting and transmitting certain information from the mobile device to third parties including ad networks. This information includes precise geolocation information and persistent device identifiers that can be used to track a user's location over time.

The app ran into two problems with these alleged data collection and use practices. First, the FTC alleged that it did not adequately disclose that information including geolocation and the persistent device identifiers would be collected and shared with third parties, such as advertising networks. Second, the app did not accurately represent consumers' choices with regard to the collection, use and sharing of this information.

However, the Complaint does not start out by focusing on these collection and use practices, and the app's disclosures relating to them. Instead—and not insignificantly—it starts by describing the app's promotional page on the Google Play store. The Complaint notes that this page describes the flashlight app, but "*does not make any statements relating to the collection or use of data from users' mobile devices*" (emphasis added). Similarly, the FTC notes that the general "permission" statements that appear for all Android applications provide notice about the *collection* of sensitive information, but not about any *sharing* of sensitive information. But these issues do not reappear in the FTC's allegations regarding the actual violations of Section 5 of the FTC Act for deceptive practices. Thus, it seems safe to assume that the FTC cited the lack of notice *prior to download* about the use and sharing of sensitive information to signal to app developers and platforms that it expects to see such disclosures.

THE APP'S DISCLOSURES REGARDING SENSITIVE DATA

The FTC's allegations specifically focus on the disclosures made by the app in its privacy policy and end user license agreement ("EULA"). In short, the Complaint notes that while the app's privacy policy discloses that the app collects information relating to "your computer," it does not *specifically disclose*: (1) that sensitive information such as precise geolocation is collected; or (2) that it is transmitted to third parties. Based on this failure to disclose, the FTC alleged that the app violated Section 5 by materially misrepresenting the scope of its data collecting and sharing, specifically the collection and sharing of precise geolocation information and persistent device identifiers.

As for the EULA, the Complaint explains that after a user downloads and installs the app, the user is presented with a EULA that must be accepted to use the app. First, like the privacy policy, the FTC alleges that the EULA does not accurately and fully disclose the data and sharing practices of the app. Second, the FTC alleges that the EULA also misleads consumers by giving them the option to "refuse" its terms. As the Complaint puts it, "that choice is illusory." The problem is that the app transmits device data including precise geolocation and the persistent identifier before the user accepts—or refuses—the terms of the EULA. As a result, the EULA misrepresented that consumers had the option to "refuse" the collection of this information, because "regardless of whether consumers accept or refuse the terms of the EULA, the Brightest Flashlight App transmits . . . device data as soon as the consumer launches the application…"

NEW DISCLOSURES REQUIRED BY THE SETTLEMENT

For the most part, the **Agreement and Consent Order** is what we've come to expect from the FTC in Section 5 cases relating to data collection and use practices. Thus, for instance, Goldenshores and any apps it develops, including this Flashlight app, are barred from misrepresenting the manner in which information is collected, used, disclosed or shared.

What makes this Order unique, however, is the specificity the FTC provides with regard to the disclosures Goldenshores must make about the collection and use of precise geolocation information in its apps. The Order requires a notice that

goes significantly beyond the typical boilerplate "just-in-time" opt-in notice that apps typically use to obtain consent for the collection of precise geolocation information. In this case, **the separate out-of-policy just-in-time notice and opt-in consent that the app must provide *prior* to collecting precise geolocation information must include a disclosure that informs the user:**

(1) That the application collects and transmits geolocation information;

(2) How this information may be used;

(3) *Why* the application is accessing geolocation information; and

(4) The identity or specific categories of third parties that receive geolocation information directly or indirectly from the app.

CONCLUSION

Thus, what looks at first to be a simple privacy policy FTC deception case is actually rather significant for three reasons. First, this is about the failure to disclose collection and use practices relating to "sensitive data," which includes precise geolocation *and* the device's unique identifier. Second, the FTC flagged the lack of disclosures about such collection and use practices in the app store prior to download. And third, the FTC gave very specific and detailed instructions to the app on how it must provide notice and choice about the collection of precise geo-location information, which could perhaps be an indication of where the FTC expects the entire industry to go in the near future.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.