May 12, 2014

Snap Judgment: FTC Alleges Snapchat Did Not Keep Its Privacy and Security Promises, Reinforces Duty to Heed 3rd Party Warnings

By D. Reed Freeman, Libby J. Greismann and Adam J. Fleisher

Snapchat's recent settlement with the Federal Trade Commission (FTC) generally provides a comprehensive but not groundbreaking roadmap to the FTC's privacy and data security expectations in the mobile environment under Section 5 of the FTC Act, with two very notable exceptions:

1. Companies are clearly required to follow researchers' direct warnings to see if there are any privacy or data security vulnerabilities, and to act on any such information promptly; and

2. We do not see any real limiting principle between this "duty" and a duty to stay up to date on widely read or on topic writings, warnings, blogs, etc., not sent directly to the company. A "knowing" standard is a very short analytical leap to a "should have known" standard. Indeed, such a case alleging failure to heed widely publicized warnings could be the next case in this line, which also includes the Credit Karma and Fandango settlements.

3. It also appears that the FTC expects companies to be aware of all third parties who have technology that can interact with an app, and to make sure that when consumers engage in any such interaction, all of the company's privacy and data security representations remain true. If the FTC continues down this path, it will create unsustainable new burdens on app developers, many of which have very few resources to begin with. Furthermore, if this is the new standard, there is no reason it should be limited to the app environment—analytically, this would lead to a rule of general application.

THE BASIC ALLEGED MISREPRESENTATION

The Snapchat app became very popular because of its branding as an "ephemeral" mobile messaging service. Among other things, the app promised its users and prominently represented—in its privacy policy and an FAQ, among other places—that the "snaps" (e.g., messages) users sent would "disappea[r]

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Peter Day (650) 813-4231
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
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
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
D. Reed Freeman, Jr. (202) 887-6948
Libby J. Greisman (202) 778-1607
Julie O'Neill (202) 887-8764
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
Amy Collins 44 20 79204180
Susan McLean 44 20 79204045

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
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

forever" after 10 seconds (or less). However, according to the FTC's complaint, in addition to other problems with the app's privacy and security features, it was much too easy to capture these supposedly ephemeral messages, making the company's claims false and misleading in violation of Section 5. And since the company's representations were not consistent with the app's practices, now it's the FTC that won't be disappearing any time soon.

A NEW DUTY TO DISCOVER POSSIBLE VULNERABILITIES

Given the app's popularity, along with its unqualified claims ("snaps disappear . . ."), maybe it shouldn't be surprising that creative users and other opportunistic individuals found ways to preserve these supposedly fleeting messages. As the FTC complaint put it, "several methods exist by which a recipient can use tools outside of the application to view and save snaps indefinitely." The FTC noted in particular "widely publicized" methods for saving video files sent through Snapchat and for using smartphones' "screenshot" functionality to capture a snap. The FTC further alleges that Snapchat was aware of a more generalized potential problem. "As early as June 2012, a security researcher warned Snapchat that it would be pretty easy to write a tool to download and save images a user receives due to the way the API functions" (complaint at paragraph 11). With regard to the screenshot work-around, Snapchat also represented that the app would "let you [the sender] know if [recipients] take a screenshot." But this representation was allegedly misleading because of the well-known means for circumventing the app's alert mechanism.

But the FTC also seems to have collapsed a subtly different type of problem with the app into the discussion of these allegedly "widely publicized," albeit ad hoc, means to preserve supposedly ephemeral snaps. As the complaint (and press release) put it, a "security researcher" warned the company in 2012 that the way its API[1] functioned made it possible for third-party apps to download and save photo and video messages sent through the Snapchat service, since the deletion function was wholly dependent on the Snapchat application itself.

According to the FTC, this "warning" to Snapchat should have been sufficient to put the company on notice that its app had a vulnerability. It also begs the question whether companies have a new "duty to discover" potential privacy or security vulnerabilities. It's one thing for this type of flaw to lead to a misrepresentation based on the ephemeral nature of the snaps (since Section 5 is a strict liability statute, and Snapchat's representations allegedly were facially misleading), but it would be quite unprecedented for the FTC to create a duty to be aware of (and therefore respond to) the warnings of "security researcher[s]," especially if those warnings are not "widely publicized," or received by the company, or credible, from the company's perspective.

There is, of course, no guidance in the Snapchat settlement about *which* researchers companies may need to pay attention to, or which warnings they must quickly heed. The FTC may be heading down a road where they take the position that Section 5 requires app developers to proactively monitor the online community for possible security vulnerabilities. There is also no analytical reason to limit this new expectation to app developers. As a result, if the FTC takes this next step, it risks creating considerable compliance costs for all kinds of companies, and not just mobile app companies.

ADDITIONAL SECTION 5 VIOLATIONS – A CHECKLIST FOR MOBILE APP COMPLIANCE

Geolocation. The complaint also alleges that the company deceived users about the amount of personal data it collected, and about the security measures in place to protect that data. Until February 2013, Snapchat's privacy policy claimed that

[1] Application programming interface.

the app did not ask for, track, or access any location-specific information from users' devices at any time. However, according to the FTC, Snapchat integrated a third-party analytics tracking service in October 2012 that collected users' WiFi-based and cell-based location information from the app.

Accessing contacts. The privacy policy further claimed that the app only collected users' email, phone number, and Facebook ID for its "Find Friends" feature, which is a way to find other users of the app. But Snapchat collected the names and phone numbers of all contacts in the users' mobile device address book who utilized the Find Friends feature.

Reasonable security. The last count of the complaint alleges that the company failed to secure the Find Friends feature, both by: failing to verify that the phone number that a user entered did, in fact, belong to the mobile device being used by that individual; and by failing to implement restrictions on the number of Find Friend requests that any one account could make. Hackers were allegedly able to exploit flaws in the app's security to access 4.6 million Snapchat usernames and phone numbers. In light of these vulnerabilities, the FTC alleged that the company's representations about how it secures users' data (e.g., "Snapchat takes reasonable steps to help protect your personal information") were false and misleading as well.

Privacy by design. As the FTC has made clear, developers must implement privacy-by-design by building privacy and security into the app's structure from the outset. A privacy-by-design program should address privacy risks, protect the privacy and confidentiality of personal information, and provide policies and procedures sufficient to cover the nature and scope of the app and the sensitivity of the information collected.

* * *

The FTC's allegations in the Snapchat complaint epitomize the FTC's ongoing and broadening efforts to ensure that companies market their apps truthfully and protect user information. For an app to be in compliance with Section 5, it is clear that: (1) consumer controls must work for every consumer, every time, under all conditions and use cases, *even ones that the developer is unaware of*; (2) collection of information from users' address books requires clear disclosure and an opt-out preference; and (3) representations about "reasonable" security create specific legal obligations to protect user data, just as representations about privacy create legal obligations to use information in a manner consistent with those representations.

But given the way that the Snapchat app interacted with third-party apps, and the FTC's allegations relating to those interactions, the Snapchat settlement also suggests that: (1) app developers need to pay attention to privacy and data-security bloggers, and promptly remedy bugs found by these third parties; and (2) representations about which data is or is not collected by an app must extend to third-party tools that can use information generated by the users of that app.

CONCLUSION

Though in many ways the FTC's complaint and consent order are similar to those the FTC has issued recently, the settlement is significant because of its breadth.

The Snapchat app itself illustrates current expectations of consumer controls, as well as the notion of privacy as a marketable concept in its own right. The app's popularity was driven by the idea of privacy itself as a desirable commodity. But, according to the FTC, the app couldn't deliver on its unqualified promises, and that made it a fairly easy target for the FTC.

As more app developers offer consumers privacy options, they need to be certain that they can live up to the promises they make, for every user, every time, under all conditions and use cases it is also now prudent to follow researchers' "warnings" especially those sent to the company directly, and understand all use cases continuously, because the FTC's interest in mobile applications is not ephemeral.

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.