

# SociallyAware

The Law and Business  
of **Social Media**

[Home](#) > [FTC](#) > [Snap Judgment: FTC Alleges Snapchat Did Not Keep Its Privacy and Security Promises, But Suggests Broad New Duty in the Process](#)

## Snap Judgment: FTC Alleges Snapchat Did Not Keep Its Privacy and Security Promises, But Suggests Broad New Duty in the Process

By [Reed Freeman](#), [Libby Greismann](#) and [Adam Fleisher](#) on May 13th, 2014

Posted in [FTC](#), [Privacy](#)

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. It now appears that companies are required to follow researchers' blogs and other writings to see if there are any privacy or data security vulnerabilities, and to act on any such information promptly; and
2. 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] 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

**MORRISON  
FOERSTER**

### About Socially Aware

Social media sites are transforming not only the daily lives of consumers, but also how companies interact with consumers. Here at Morrison & Foerster, across all of our practice groups, we are seeing complex, cutting-edge legal issues arising out of social media. As with the Internet boom during the mid-to-late 1990s, social media is generating new legal questions at a far faster pace than the law's ability to provide answers to such questions. In an effort to stay on top of these emerging issues, and to keep our clients and friends informed of new developments, Morrison & Foerster publishes this blog devoted to the law and business of social media.

### Editors

[John Delaney](#)

[Gabriel Meister](#)

[Aaron Rubin](#)

### Contributors

[Reed Freeman](#)

[Libby Greismann](#)

[Adam Fleisher](#)

[Julie O'Neill](#)

[Patrick Bernhardt](#)

[Whitney McCollum](#)

[Craig Whitney](#)

[Nathan Taylor](#)

[John Delaney](#)

[Jay Baris](#)

### Stay Connected

 [Socially Aware on Twitter](#)

 [Socially Aware on LinkedIn](#)

in particular “widely publicized” methods for saving video files sent through Snapchat and for using smartphones’ “screenshot” functionality to capture a snap. 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 application programming interface (API) 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.

The fact that this “warning” to Snapchat—note that the complaint does *not* say *if* or *how* Snapchat *actually received or learned about this warning, if at all*, or that the warning was “widely publicized”—evidently should have been sufficient to put the company on notice that its app had a vulnerability suggests that the FTC may be trying to create a very broad “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’s quite unprecedented for the FTC to suggest a duty to be aware of (and therefore respond to) the warnings of “security researcher[s],” especially if those warnings are not “widely publicized.”

There is, of course, no guidance in the Snapchat settlement about *which* researchers companies are supposed to pay attention to, or which warnings they must quickly heed. Evidently, the FTC thinks that Section 5 requires app developers to proactively monitor the online community for possible security vulnerabilities. There is no analytical reason to limit this new expectation to app developers. As a result, the FTC 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 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.

\* \* \*

 [Subscribe to this blog via RSS](#)

 [Subscribe to this blog by email](#)

---

## Get the Socially Aware Newsletter

Enter your email below for a free subscription to Socially Aware:

---

### Topics

[Arbitration](#)

[Asia](#)

[Copyright](#)

[Crowdsourcing](#)

[Daily Deals](#)

[Discovery](#)

[DMCA](#)

[E-Commerce](#)

[E-Discovery](#)

[E-Personation](#)

[Employment Law](#)

[Ethics](#)

[Event](#)

[FCC](#)

[FDA Regulations](#)

[FEC Regulations](#)

[Federal Communications Commission Reform Act](#)

[Financial Institutions](#)

[First Amendment](#)

[FTC](#)

[Infographic](#)

[Internet of Things](#)

[Investment Management Law](#)

[IP](#)

[JOBS Act](#)

[Litigation](#)

[NAD](#)

[Online Promotions](#)

[Privacy](#)

[SEC](#)

[Section 230 Safe Harbor](#)

[Securities Law](#)

[Statistics](#)

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; follow researchers' "warnings"; and understand all use cases continuously, because the FTC's interest in mobile applications is not ephemeral.



TAGS: [Data Security](#), [FTC](#), [FTC Act](#), [Litigation](#), [mobile](#), [mobile applications](#), [Personal Information](#), [privacy](#)

0 Comments

Socially Aware Blog

d Login

Sort by Best

Share Favorite



Start the discussion...

Be the first to comment.

Status Updates

Supreme Court

Terms of Use

Trademark

UK High Court

Uncategorized

Wearable Computers

## Socially Aware on Twitter

Socially Aware: The Social Media Law Update Latest Tweets from MoFoSocMedia

Fascinating article on how Peoria mayor used police force, search warrants in effort to shutdown fake Twitter acct <http://t.co/lhSzW9RxUj> 13 hours ago

#SocialMedia Marketing Brings New Risks to #Mortgages; Audit Trail Requirements Present Challenges for Lenders <http://t.co/wcrqCYPnst> 14 hours ago

Blog post: #FTC Alleges #Snapchat Did Not Keep #Privacy & Security Promises, Suggests Broad New Duty in the Process <http://t.co/VuRc930mBI> 19 hours ago

EU court backs "right to be forgotten" in Google case; links to "irrelevant" data to be erased on request <http://t.co/xVp8H1qpdu> #privacy 20 hours ago

Should Companies Monitor Their Employees' Social Media? Two Experts Square Off: <http://t.co/b2qQMhVlH> #socialmedialaw 1 day ago

## Archives

Select Month

## Blogs

AllFacebook

ArsTechnica

CNET's "The Social"

EFF Deeplinks Blog

Louis Gray's Blog

Mashable

Social Media Examiner

Social Media Today

SocialTimes

Soshable

Techneme

Technology & Marketing Law Blog

The Facebook Blog

The LinkedIn Blog

Twitter Blog

---

## Other Morrison & Foerster Blogs

[MoFo Jumpstarter](#)

[MoFo Tech Blog](#)

[Private Surgeon General Class Action Defender](#)

[The BD/IA Regulator](#)

---

## Tags

[CDA Clickwraps Communications](#)

[Decency Act Consumer](#)

[Protection COPPA](#)

[Copyright Crowdfunding Data](#)

[Protection Data Security](#)

[Defamation Digital Millennium Copyright Act](#)

[Employment Employment](#)

[Law Europe European Union](#)

[Facebook Federal](#)

[Trade Commission FINRA First](#)

[Amendment FTC FTC Guides](#)

[Google Legislation LinkedIn](#)

[Litigation mobile Mobile](#)

[Devices NLRA NLRB Online](#)

[Contracts Personal](#)

[Information privacy](#)

[Privacy Policies SEC](#)

[Section 230 Securities Law](#)

[social media](#)

[Social Media Policies](#)

[Stored Communications Act Telephone](#)

[Consumer Protection Act Terms of](#)

[Service Terms of Use Trademark](#)

[Twitter YouTube](#)

---

## Key Moments in Social Media Law



of "one-click" shopping)

**October 28, 1998**  
The Digital Millennium Copyright Act goes into effect, establishing certain safe harbors shielding online service providers from monetary damages for copyright infringement, one of these safe harbors provides protection in connection with the hosting of user-generated content, thereby paving the way for the rise of social media.

**June 27, 2005**  
The U.S. Supreme Court decides MGM v. Grokster, holding that, where Grokster distributed its P2P file sharing software with the intention of promoting its use to infringe copyright, Grokster could not rely on protection from copyright claims under the Sony defense "substantial noninfringing use" doctrine.

**June 27, 2006**  
MySpace modifies its online terms of service in response to the opinion issued by U.S. judge-superior Billy Brynn's highly public removal of its songs from MySpace.com in protest of the website's terms of service. MySpace's revised terms of service clarified that artists retained the rights to their works, and required any MySpace request certain licenses from artists.

**February 2008**  
The Wall Street Journal sues the 2008 lawsuit against Facebook, reportedly at a value of \$65 million. The lawsuit, drafted in the name of the social network, alleged that Facebook founder Mark Zuckerberg had misappropriated the data for Facebook from Blackboard's social media website, Connect. Further, a lawsuit was reportedly filed near the settlement, and it was not until April 2011 that the Ninth Circuit brought an end to the legal wrangling, upholding the parties' 2008 settlement.

**March 2008**  
Two Texas lawyers separately sue Cisco and one of its in-house IP attorneys for alleged defamation in connection with the in-house attorney's anonymous postings on the Patent Troll Tracker Blog. The Cisco employee made the posts – alleging possible misconduct by opposing counsel in a Cisco-related patent dispute – without his employer's knowledge, but Cisco was nevertheless dragged into the litigation. In September 2008, Cisco settled with the plaintiff, a Cisco attorney four days of trial. The second lawsuit was settled on January 8, 2010.

**December 30, 2008**  
Facebook sues Power.com for collecting and re-posting Facebook user information on the Power.com website while circumventing Facebook's developer platform. After dismissal of Power.com's counterclaim against Facebook for "anticompetitive" behavior, Power.com shut down its service in April 2011, and the domain name went up for auction in July 2011.

**February 6, 2009**  
Facebook changes its online terms of service to include a broad, perpetual license to user-generated content. Twelve days later, after extensive user backlash and a threatened complaint by the Electronic Privacy Information Center, Facebook rolls back the changes.

**March 26, 2009**  
The first ever defamation lawsuit arising from a tweet is filed against Courtney Love, following a heated exchange between the rock star and a Twitter design on Twitter. The case, *Shawang v. Love*, was settled in March 2011.

**July 2, 2009**  
Lori Drew, whose online cyber-bullying behavior allegedly led to the suicide of a 13-year-old Myspace user, is acquitted of all charges. The case highlighted the perils of unregulated social networking by minors, as well as the practical limits of the Computer Fraud and Abuse Act, an anti-hacking statute that formed the basis of the prosecution's case against Drew.

**October 5, 2009**  
Revised FTC "Guides Concerning the Use of Endorsements and Testimonials" are published, addressing shady practices in connection with blogs and other social networking sites. The Guides provide that where a blogger receives free products or services from a company, and then subsequently endorses the company's products or services, the blogger must disclose the earlier received gifts. If such gifts are not disclosed, both the blogger and the company may be engaged in an unfair or deceptive practice under the FTC Act.

**May 14, 2010**  
Google announces that its vehicles used for photographing streets for Google Maps inadvertently collected personal information being transferred over open Wi-Fi networks. The collection triggered a host of class action lawsuits, as well as regulatory action in many of the 30+ countries where the vehicles were operating.

**June 23, 2010**  
The District Court for the Southern District of New York decides *Blacore v. YouTube*, finding that YouTube's loading of advertising user-generated videos is protected under one of the DMCA's safe harbors from copyright damages. Currently on appeal to the Second Circuit, a reversal could create major headaches for social media companies dependent on user-generated content to attract traffic and ad revenues.

**August 26, 2010**  
29 new Beach Communications settles FTC deceptive advertising charges for writing positive iTunes reviews for its clients' mobile apps without disclosing it was paid to promote such apps. The charges were the FTC's first enforcement action aimed at targeting the deceptive practices outlined in the 2009 revised FTC Guides.

**October 27, 2010**  
The National Labor Relations Board files a complaint against an ambulance service provider, alleging that the company illegally terminated an employee for making derogatory remarks on her Facebook page regarding her supervisor. The NLRB also alleged that the company's social media policy was overly restrictive and violated federal labor law. Although the dispute was ultimately settled, the NLRB's complaint served as a wake-up call for employers regarding the need to ensure that their social media policies do not interfere with their employees' protected legal rights.

**May 19, 2011**  
Lithtech successfully completes its initial public offering, becoming the first major U.S. social media site to be publicly traded. Other social media sites including Angie's List, Oregon, Posters, Zillow and Zillow 360 launched in Aug 2011.

**November 29, 2011**  
Facebook agrees to settle its dispute with the FTC over charges that Facebook unlawfully made its users' private profiles in December 2008. Under the FTC's proposed settlement, Facebook's privacy practices would be subject to extensive FTC oversight.

Courtesy of Socially Aware: the social media law update. Our blog is located at [www.sociallyawareblog.com](http://www.sociallyawareblog.com). You can also follow us on Twitter @SociallyAware. For a free subscription to our newsletter, please visit [www.sociallyawareblog.com](http://www.sociallyawareblog.com).

This information provided herein does not constitute legal advice, and should not be relied upon, unless your specific legal advice is based on your individual situation. This news contained herein may not be attributed to Morrison & Foerster, its attorney or clients.

We are Morrison & Foerster – a global firm of exceptional talent in many areas. Our clients include some of the largest financial institutions, Fortune 500 companies, government bodies and technology and life sciences companies. Our clients count on us for strategic and business-critical solutions. Our commitment to serving client needs has resulted in lasting relationships and a record of high achievement. For the best legal advice, we're located in over 40 offices around the world. For more information, visit [www.morrisonfoerster.com](http://www.morrisonfoerster.com) or call 1-800-345-2688. Our attorneys are committed to achieving results for our clients, while preserving the differences that make us change. This is who we are.

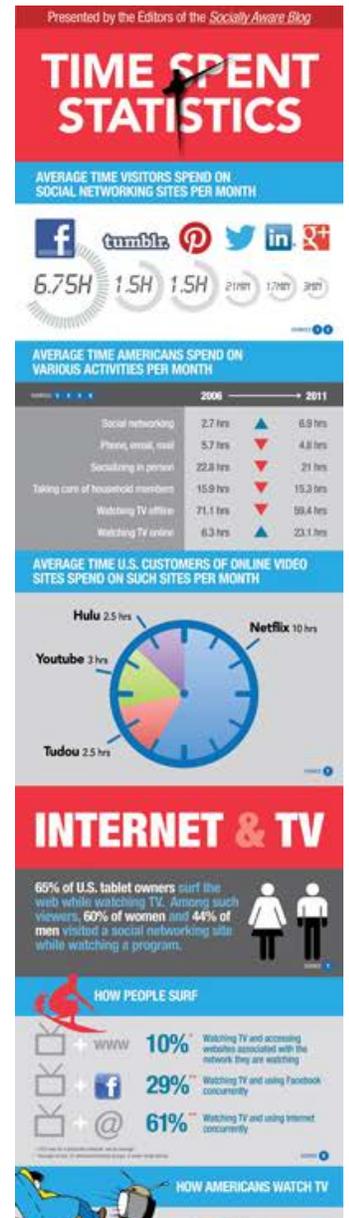
**MORRISON | FOERSTER**

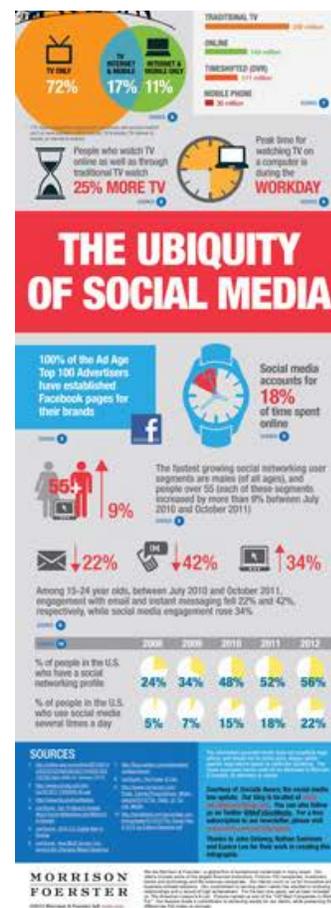
©2012 Morrison & Foerster LLP. All rights reserved.

## A Short History of Social Media



## The Growing Impact of Social Media





## Socially Aware Blog

### Morrison & Foerster LLP

BEIJING | BERLIN  
BRUSSELS | DENVER  
HONG KONG | LONDON  
LOS ANGELES | NEW YORK  
NORTHERN VIRGINIA | PALO ALTO  
SACRAMENTO | SAN DIEGO  
SAN FRANCISCO | SHANGHAI  
SINGAPORE | TOKYO | WASHINGTON DC

#### Stay Connected



#### About MoFo

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, Chambers Global named MoFo its 2013 USA Law Firm of the Year, and Chambers USA named the firm both its 2013 Intellectual Property and Bankruptcy Firm of the Year. In addition, BTI named MoFo among its 2013 Brand Elite. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger.

The views expressed herein shall not be attributed to Morrison & Foerster, its attorneys or its clients.

#### Recent Updates

[Snap Judgment: FTC Alleges Snapchat Did Not Keep Its Privacy and Security Promises, But Suggests Broad New Duty in the Process](#)

[Complimentary JOBS Act Seminar](#)

[If You Host Videos on Your Website, Read This Blog Post Regarding the Video Privacy Protection Act](#)

[Which Way is Aereo Pointing? The Supreme Court Hears Arguments in Public Performance Copyright Case](#)

[Next Generation State Privacy Law: Regulating the Commercial Use of Drones](#)

[Hot Off the Press: The April Issue of Our Socially Aware Newsletter Is Now Available](#)

[Jerked Around? Did the FTC's "Jerk.com" Complaint Just Turn API Terms Into Federal Law?](#)

[New Regulatory Guidance on Use of Social Media by Investment Advisers](#)

