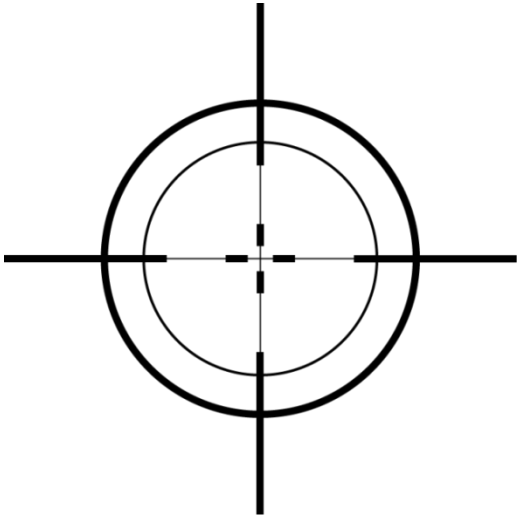
Staying Out of Trouble:

Avoiding Privacy, Data Security, and Advertising Mistakes That Can Put You in the Enforcement Crosshairs



May 21, 2015

Reed Freeman

Heather Zachary

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

Attorney Advertising

Speakers

Reed Freeman
Partner
WilmerHale

Heather Zachary
Partner
WilmerHale

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and 1.0 non-transitional CLE credit in New York*
- WebEx customer support: +1 888 447 1119, press 2

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. Attendees requesting CLE credit must attend the entire program.*

Overview

- The FTC: Privacy and Deception/Unfairness
- Avoiding Trouble While Advertising: Mobile and More
- Data Security Compliance and Enforcement
- State-Law Traps for the Unwary
- New Cops on the Beat: The Consumer Financial Protection Bureau and the Federal Communications Commission
- Other Recent Developments (including the "Internet of Things" and Litigation Trends)
- Key Take-Aways
- Questions

Privacy and the FTC Act: Deceptive and Unfair Trade Practices

Section 5 of the FTC Act: A Primer

The FTC Act prohibits **deceptive** practices in the marketplace

- A trade practice is "deceptive" under the FTC Act when:
  - there is a representation, omission, or practice likely to mislead consumers;
  - the consumers are acting reasonably under the circumstances; *and*
  - the representation, omission, or practice is material.
- Deceptive trade practices include:
  - collecting data in a manner that is inconsistent with statements made in a privacy policy or elsewhere
  - sharing information with third parties despite contrary promises
  - making misleading statements in advertising about your (or another's) service

Section 5 of the FTC Act: A Primer

The FTC Act also prohibits **unfair** practices in the marketplace

- A trade practice is "unfair" within the meaning of the FTC Act when:
  - it causes or is likely to cause substantial injury to consumers;
  - the injury is not reasonably avoidable by consumers; *and*
  - the injury is not outweighed by benefits to consumers or to competition.
- Unfair trade practices include:
  - failure to provide adequate security for sensitive consumer data
  - engaging in expansive and/or intrusive tracking of consumers without providing adequate notice or choice

FTC: Privacy Cases

Over the past 20 years, the FTC has brought actions addressing a wide variety of privacy violations:

- Third-party data sharing
- Spyware or tracking mechanisms
- Spam and telemarketing
- Failure to honor privacy promises
- Omission of key facts from privacy policies
- Partnerships with companies that obtain data illegally

Let's review some of the FTC's recent cases for key compliance and enforcement lessons…

Spotlight on: Snapchat, Inc.

132 3078

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Edith Ramirez, Chairwoman
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Terrell McSweeny

In the Matter of	)	DOCKET NO.
Snapchat, Inc., a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that Snapchat, Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Snapchat, Inc. ("Snapchat"), the successor corporation to Toyopa Group LLC, is a Delaware corporation with its principal office or place of business at 63 Market Street, Venice, California 90291.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

"However, when the user chooses to Find Friends, Snapchat collects not only the phone number a user enters, but also, without informing the user, the names and phone numbers of all the contacts in the user's mobile device address book."

Snapchat: FTC's Allegations

Highlights:

- Recipients could save "snaps" indefinitely, contrary to Snapchat's claim they would "disappear forever"
- Snapchat collected location information about the users, despite representations to the contrary
- Snapchat collected contact information stored on mobile phones without notice or consent
- Insecure security measures allowed a breach that resulted in attackers compiling a database of 4.6 million usernames and phone numbers

Beware of Making and Breaking Promises

The FTC has brought numerous other cases alleging falsity of promises that companies have made to consumers about their data.

- **Brightest Flashlight**: claimed to collect certain information purely for internal housekeeping purposes, then sold it to third-party advertisers.
- **Scan Scout**: provided an opt-out for certain cookies but still tracked consumers with other cookies.
- **Epic Marketplace**: claimed to limit the nature of its tracking but used history-sniffing technology to track consumers across the web – including when they visited financial and health websites.
- **Path**: collected personal data from users' mobile device address books, contrary to statements in privacy policy.
- **Nomi**: retail location-tracking service misled consumers with promises that it would clearly indicate when it was operating and would provide an in-store mechanism for consumers to opt out. Violation found even though promises went beyond what the law required.

Make Clear and Conspicuous Disclosures

The FTC has established in enforcement actions and guidance that merely providing accurate disclosures about your privacy practices is not enough. Disclosures also must be sufficiently *clear* and *conspicuous* to enable consumers to have actual notice of your practices.

- **Sears**: Though Sears disclosed its tracking, it buried its disclosures deep in a "scroll box" that let consumers see only 10 lines of text at a time.
- **Advertising.com**: Offered free security software, and failed to disclose adequately that adware was bundled with that software. Notice appeared in a licensing agreement that consumers were not required to read.
- **FTC ".com Disclosure Guidance"**: Provides specific guidance about how to make effective disclosures in digital advertising.
- **Point-of-collection disclosures**: Provide notice of data uses and sharing at the point where the information is collected.
- **Point-of-use disclosures**: Provide notice "just in time" as the data is being processed (e.g., icon that appears when location tracking is in use).

The FTC's Privacy Principles

Privacy by Design

- Reasonable data collection and retention limits
- De-identification of data where feasible; effective policies to not re-identify it
- Sound data security and disposal practices

Increased Transparency

- Privacy policies that are easy-to-read and easy-to-understand
- Provide additional notices at the time the consumers are providing their data

"Usable" Choices

- Easy-to-exercise choices
- Limit data usage to what is appropriate given the relationship with the consumer

Avoiding Trouble While Advertising: Mobile and More

Key Mobile Advertising Dos and Don'ts

- **DO:** If retargeting or using Interest Based Advertising, use the "Advertising Options" Icon.
- **DO:** Make opt-out deterministic, which is hard on mobile devices because cookies don't work well.
  - Use the new DAA App Choices program or something similar to make sure that mobile opt-out works and is persistent.
- **DON'T:** Ignore the terms of use for Google and Apple Ad IDs. There is precedent for FTC liability under Section 5 for failing to heed such terms.
- **DON'T:** Engage in cross-device tracking without notice from the landing page of the "Advertising Options" Icon that you're doing so, and a deterministic opt out. If possible, make opt-out of one device = opt out of all devices.
- **DON'T:** Engage in the use of Stat IDs without a deterministic opt-out.

Text Messaging Dos and Don'ts Under the TCPA

- The **Telephone Consumer Protection Act ("TCPA")** regulates telemarketing and the use of automated telephone equipment for voice calls, faxes, and text messages.
- The TCPA provides for a private right of action and colossal statutory damages, making it a favorite of class-action plaintiffs: up to $1,500 *per recipient* for *each text message* sent.
- Consent is required for any text message, and for commercial messages "prior express written consent" is required.
  - Clearly and conspicuously disclose that the recipient is authorizing delivery, to the designated phone number, of marketing text messages.
  - Clearly and conspicuously disclose that the recipient need not agree to receive text messages as a condition of purchasing any property, good, or service.
  - Obtain clear opt-in consent (e.g., through un-checked box) and retain proof.
  - There is *no exception* for a pre-existing business relationship.
- The consent requirements are somewhat relaxed for non-commercial text messages, but reliance on this exception can be risky.

Text Messaging Dos and Don'ts Under the TCPA

- Send a text message to the mobile device that requires the recipient to activate his or her sign-up before receiving any further text messages.
- Include on the sign-up screen, in the confirmation text message, and wherever possible in substantive text messages:
  - instructions for unsubscribing from messages by replying with "STOP"
  - instructions for obtaining customer service support by replying with "HELP"
  - a statement warning that "Msg & Data Rates May Apply"
- For all text messages, clearly disclose that you are the sender.
- Honor unsubscribe requests *as soon as possible* – ideally within five minutes.
- Additional requirements apply in other jurisdictions (e.g., Canada).

Email Dos and Don'ts for the U.S. and Canada

- **CAN-SPAM Act**. Governs content and other features of "commercial electronic mail messages" (namely, emails whose primary purpose is advertising or promoting a commercial product or service)
  - Mandatory opt-out mechanism for commercial e-mail
  - Exceptions for transactional & relationship messages
  - Emails must contain the identity and mailing address of the sender
  - Penalties for violations of up to $16,000 *per email*
- **Canada's Anti-Spam Legislation ("CASL")**. Governs content and other features of emails, texts, and other "commercial electronic messages." It is stricter than the CAN-SPAM Act in many respects.
  - Express, ***opt-in*** consent generally is required to send commercial messages
  - Imposes content and other requirements for even *transactional* messages, including a link to the company's opt-out mechanism
  - Emails must include postal address *and* telephone number or website address or email address
  - Penalties of up to $10 million, as well as *personal* liability and criminal charges

Email Dos and Don'ts for Canada and the EU

- CASL provides exceptions to the opt-in consent requirement, including:
  - Messages sent in certain existing business relationships
  - Responses to an inquiry, request, or complaint
  - Initial messages sent subsequent to a referral
  - Some messages sent to disclosed or published addresses

- CASL went into effect less than a year ago, but Canadian regulators are enforcing it already (including through a $1.1 million fine).

- **EU E-Privacy Directive, Art. 13 (2002/58/EC)**.
  Imposes requirements with respect to emails, texts, and other messages used for direct marketing.

  - Consent required for direct marketing messages
  - Business relationship exception where a customer provides an email address "in the context of the sale of" a product or service, and the address is used to directly market the company's "own similar products or services"
  - Customers must "clearly and distinctly [be] given the opportunity to object, free of charge and in an easy manner, to" marketing emails when their address is collected and "on the occasion of each message"

Data Security Compliance and Enforcement: The FTC Act and More

FTC: Data Security Cases

The FTC Standard: Administrative, technical, and physical controls to protect against reasonably foreseeable threats to the security, confidentiality, and integrity of consumers' personal information, taking into account the size and complexity of the company, the nature of its activities, and the sensitivity of the data.

Recent Cases

- **GeneLink**: failed to protect consumer information such as genetic information, Social Security numbers, bank account information, and credit card numbers.
- **GMR Transcription Services**: allowed patients' medical histories and other information to be indexed on an Internet search engine.
- **Twitter**: allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information, and to send tweets from user accounts (including one from President Obama).

Spotlight on: TRENDnet, Inc.

In the Matter of

TRENDNET, INC.,
a corporation.

DOCKET NO. C-4426

COMPLAINT

The Federal Trade Commission, having reason to believe that TRENDnet, Inc., a corporation, has violated the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent TRENDnet, Inc. ("TRENDnet" or "respondent") is a California corpo its principal office or place of business at 20675 Manhattan Place, Torra 90501.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Respondent is a retailer that among other things, sells networking devices, such as routers, modems, and Internet Protocol ("IP") cameras, to home users and to small- and medium-sized businesses. In 2010, respondent had approximately $64 million in total revenue, and obtained approximately $6.3 million of this amount from the sale of IP cameras. In 2011,

"Among other things, these compromised live feeds displayed private areas of users' homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."

TRENDnet: The FTC's Allegations

- Failure to adequately train employees to handle/dispose of information securely
- Failure to employ a reasonable process to discover risk to personal information
- Failure to use reasonable means to look for or prevent unauthorized activity
- Transmitting/storing personal information in clear text/failing to encrypt personal data/credentials
- Allowing users to bypass authentication by going to a specific URL

Key Data Security Program Components

Administrative

- Written Information Security Program (WISP)
- Training
- Vendor oversight
- Incident Response Plan

Technical

- Use reasonable available defenses
- Access control
- Secure credentials
- Encryption
- Monitoring and logging activity

Physical

- Clean desk / clean screen
- Limit access to sensitive areas and paper records
- Secure data disposal

State Laws and Enforcement

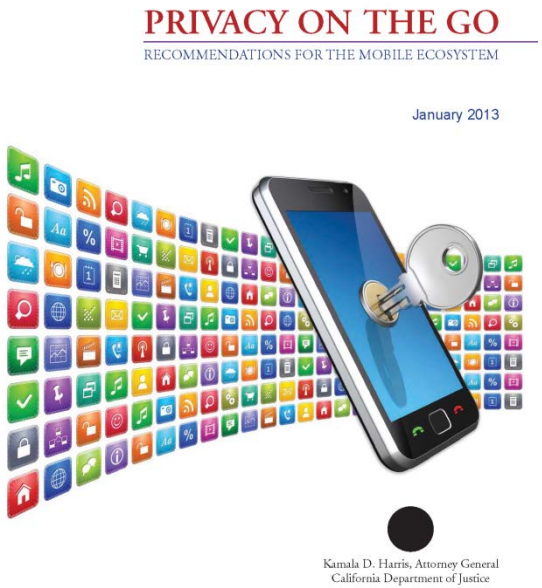
California Online Privacy Protection Act

California amended the California Online Privacy Protection Act (CalOPPA), and many companies are not yet in compliance.

- California law has long required Internet websites to provide an online privacy policy. *See* Cal. Bus. & Prof. Code §§ 22575 *et seq.*
- The Attorney General has clarified that the law applies to mobile apps too.
- CalOPPA was amended recently to require disclosure of even more info:
  - whether other parties may collect information about users' online activities over time and across different Web sites
  - how the operator responds to Web browser 'do not track' signals or other similar mechanisms
- The California AG has sued to enforce CalOPPA (against Delta Airlines). That litigation was dismissed for non-privacy reasons.

California's Mobile Privacy Recommendations

- In 2013, California issued a report with mobile privacy recommendations for app developers, app platform providers (*e.g.*, app stores), advertising networks, and others.
- Some of the recommendations in the California report go beyond existing law and are merely "best practices" rather than clear legal requirements.
- *Privacy on the Go: Recommendations for the Mobile Ecosystem*
  http://www.oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf?



Take-Aways from the California AG's Report

Do:

- Make your privacy policy accessible from within the app and in the app store so users can read it before they download your app
- Use shorter privacy disclosures and other measures to draw attention to data practices that may be unexpected
- Enable meaningful choices about the collection and use of data
- Augment disclosures when collecting sensitive data, text messages, call logs, contacts, or using sensitive device features (e.g., cameras, microphones, location tracking)

Do Not:

- Collect personally identifiable data that is not necessary for the functions of the app
- Use out-of-app ads delivered by modifying browser settings or placing icons on the mobile desktop
- Use static, device-specific identifiers for advertising

Other State-Law Traps for the Unwary

- Expansion of **state data breach laws**:
  - The scope of protected information has expanded. Florida, California, and Nevada now treat "online account" login credentials as sensitive personal information, the breach of which triggers reporting obligations.
  - Remediation obligations also have expanded.
- Specific **state data security requirements**:
  - 201 C.M.R. § 17.00 *et seq.*
  - N.Y. Gen. Bus. Law § 399-dd(1)
  - Cal. Civ. Code § 1798.85
  - Nev. Rev. Stat. § 603A.215
- **"Shine the Light" law** – California law governing marketing
- **Song-Beverly Credit Card Act** and similar state laws
  - Zip code class-action litigation
- Electronic **eavesdropping and surveillance laws** requiring all-party consent

New Cops on the Privacy and Data Security Beat

New Cops: Consumer Financial Protection Bureau

- The Dodd-Frank Act gave the **Consumer Financial Protection Bureau ("CFPB")** authority over financial institutions and other "covered persons" involved in providing a "consumer financial product or service."
- **Section 1031** of the Dodd-Frank Act bars covered persons and their service providers from engaging in any "**unfair, deceptive, or abusive act or practice** . . . in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service." 12 U.S.C. § 5531(a).
- The CFPB views this language as giving it, like the FTC, authority to police privacy and data security. Indeed, the "abusive" language does not appear in Section 5 of the FTC Act and may provide broader authority.
- The CFPB has been aggressive in performing its consumer protection role under Section 1031, and there are signs that it will do the same with respect to privacy and data security.

cfpb Consumer Financial Protection Bureau

New Cops: Federal Communications Commission

- Calling the Federal Communications Commission a "new cop" is something of a misnomer.
  - The FCC has long policed the privacy and security of consumer information through Section 222 of the Communications Act and its Customer Proprietary Network Information (or "CPNI") rules.
  - The CPNI rules govern use and disclosure of information about consumers' use of telecommunications services, including location information.
- But the scope of the FCC's authority recently expanded.
  - Section 222 and the CPNI rules apply to "telecommunications carriers" and "telecommunications services," which historically has limited their application to entities that provide telephone service and related services.
  - Under the FCC's recent net neutrality order, the CPNI rules also will apply to Internet service providers, and potentially a much larger range of entities.
- The FCC has clearly expressed an intention to regulate privacy *and* security.
  - The FCC levied a $10 million fine against two companies for lax data security.
  - Chairman Tom Wheeler has been vocal about the Commission's intention to play a significant role with respect to cybersecurity.

Other Recent Developments in Privacy and Data Security Enforcement

"Internet of Things": Risks and Recommendations

- The FTC has been very focused on the "Internet of Things." It issued a report earlier this year, and FTC Commissioners have been highlighting the Internet of Things as a high priority in 2015.
- Risks:
  - Unauthorized parties can gain access to, and misuse, sensitive consumer personal information
  - Breaches facilitate attacks on other systems
  - Data disclosures can create risks to personal safety (e.g., eavesdropping, location monitoring)
- FTC Recommendations:
  - Congress should enact strong, flexible, and technology-neutral legislation
  - Make devices more secure at outset
  - Retain service providers who can maintain security and exercise oversight
  - Ensure data minimization
  - Provide consumers with notice and choice

Recent Trends in Privacy and Security Litigation

- Data breaches
  - Unauthorized access to and misuse of personal information
  - Failure to notify in timely manner
- Disclosure of information by video streaming providers (litigation under the Video Privacy Protection Act)
- Mobile applications and location privacy
  - Recent FTC enforcement actions and consumer class actions against Accuweather.com, Fandango, Credit Karma, and Snapchat
- Regulators fueling derivative suits
- Overpayment theory of liability in data security litigation
  - Unjust enrichment
- Breach of confidentiality theory of liability
  - Duty of confidentiality and invasion of privacy

Key Take-Aways

- Develop a privacy policy and honor it
- Be honest and transparent
- Disclose, disclose, and disclose again
- Avoid missteps when advertising through mobile devices, text messages, and email

- Develop a reasonable data security program
- Keep on top of evolving state laws, litigation trends, and developments in the "Internet of Things"
- Pay attention to enforcement trends and guidance from emerging regulators

Thank You and Contact Information

Reed Freeman
Partner; Co-Chair
Cybersecurity, Privacy and Communications Practice
WilmerHale

+1 202 663 6267
Reed.Freeman@wilmerhale.com
http://www.wilmerhale.com/Reed_Freeman/

Heather Zachary
Partner
WilmerHale

+1 202 663 6794
Heather.Zachary@wilmerhale.com
http://www.wilmerhale.com/Heather_Zachary/

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. Attendees requesting CLE credit must attend the entire program.*