Current Trends and Recent Developments in FTC Privacy Enforcement

July 14, 2016

Reed Freeman
Patrick Bernhardt
Elizabeth D'Aunno

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

Attorney Advertising

Speakers

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

Patrick Bernhardt
Associate
WilmerHale

Elizabeth D'Aunno
Associate
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 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 of this program also may be able to claim England & Wales Unaccredited CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*

Agenda

- FTC privacy enforcement “101”
- Recent developments at the Commission
- Online tracking and targeting
- Mobile privacy
- Sensitive health and children’s information
- Internet of Things, Big Data, and the Fair Credit Reporting Act
- Enforcement of international frameworks

FTC Privacy Enforcement "101"

- **FTC has broad jurisdiction over companies engaged in commerce in the United States, with the exception of banks and a handful of other entities**
- **The Commission may bring actions under Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices"**
  - A practice is "**unfair**" if it causes substantial harm to consumers, is not reasonably avoidable by consumers, and is not outweighed by countervailing benefits to consumers or competition
  - A practice is "**deceptive**" if it constitutes a representation, omission, or practice that is likely to mislead consumers, acting reasonably under the circumstances, to the consumer's detriment
- **FTC also enforces sector-specific privacy laws, including COPPA, GLBA, FCRA, and CAN-SPAM**
- **The Commission has brought over 500 privacy and data security actions and recently increased the maximum civil penalties for certain violations**

"Increasingly, privacy has moved from a simple matter of legal compliance, best left to lawyers and IT professionals, to a C-suite issue – part of a broader bottom line strategy as consumer awareness and demand for privacy continues to grow"

Jessica Rich—Director, FTC Bureau of Consumer Protection

Recent Developments at the Commission

FTC's Evolving Role as Lead Privacy Regulator

- **On January 12, 2015, President Obama delivered a speech on privacy priorities to mark the 100th anniversary of the FTC**
- **Recent remarks by Commissioner Maureen Ohlhausen have emphasized the FTC's leadership role in the privacy arena:**
  - "Despite rumors to the contrary, the FTC is the primary privacy and data protection agency in the U.S." (Mar. 23, 2016)
- **Two Commissioners resigned in the past year**
  - Joshua D. Wright (August 2015)
  - Julie Brill (March 2016)
  - Only three FTC commissioners at present—two Democrats and one Republican

Increased FTC Focus on Privacy Research

The FTC increasingly has focused on conducting its own investigative research and has sought external assistance to identify and address the privacy and security implications of emerging technologies

- **Appointed new Chief Technologist, Lorrie Cranor, in December 2015**
  - Advises the Commission on new technologies and platforms to guide its enforcement and policy work (*see* Tech@FTC blog)
- **The FTC held its first-ever "PrivacyCon" event in January 2016 to explore research on privacy and security topics**
  - Designed to encourage collaboration among leading whitehat researchers, academics, industry representatives, consumer advocates, and the government
  - Next PrivacyCon event scheduled for January 12, 2017, and the FTC has invited researchers to submit research on a variety of issues

"It is extremely valuable for us to hear from privacy and security researchers about their work. This helps us stay up-to-date with technology **and identify potential areas for investigation and enforcement.**"

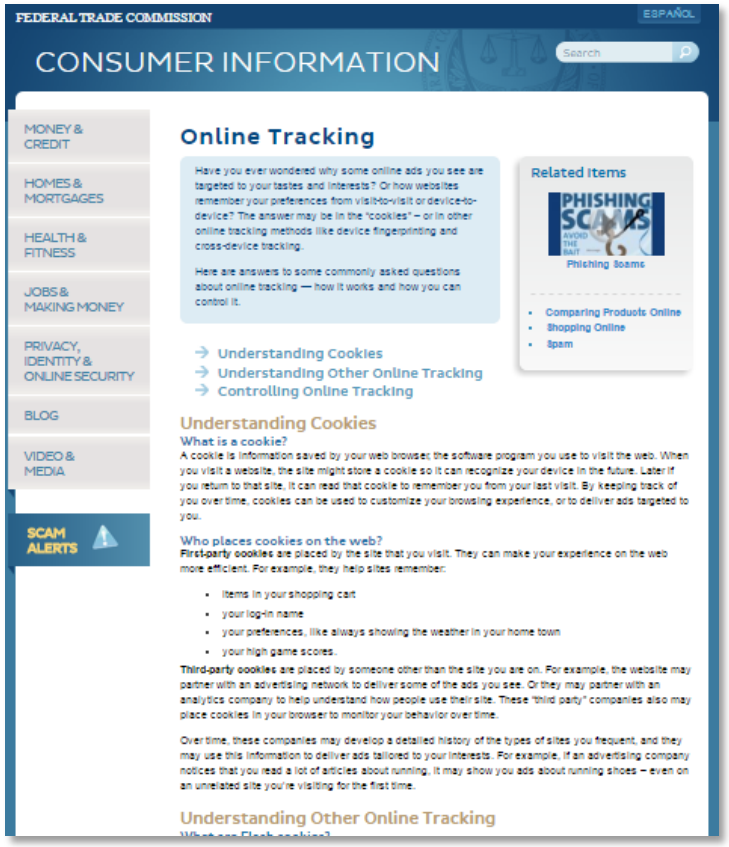
Lorrie Cranor, FTC Chief Technologist

FTC "Fall Technology Series" and Upcoming Workshop

- **Ransomware (Sept. 7, 2016)**
  - Explore how to reduce risks, respond to incidents, and decrease harm
- **Drones (Oct. 13, 2016)**
  - Determine how businesses, self-regulatory groups, and foreign regulators are addressing privacy concerns and whether there is a need for FTC guidance
- **Smart TV (Dec. 7, 2016)**
  - Understand new tracking and advertising technologies on smart TVs, streaming devices, game consoles, apps, and set-top boxes (a.k.a. "addressable TV"), and how they are used to deliver relevant advertising on TVs and other devices
  - Identify best practices—and potentially issue FTC guidance—on addressable TV
- **"Putting Disclosures to the Test" (Sept. 15, 2016)**
  - Explore how to test privacy-related disclosures, including privacy policies and other mechanisms, to inform consumers that they are being tracked

Online Tracking and Targeting

Updated Consumer Guidance for Online Tracking



Highlights various types of online tracking:

1. First-party and third-party cookies
2. Flash "cookies"
3. Device fingerprinting
4. Mobile device identifiers
5. "Smart device" tracking on TVs, game consoles, and streaming devices

Explains how consumers can control tracking:

1. Block or reset cookies, use private browsing mode, or use ad blockers
2. Disable Flash "cookies"
3. Reset or change preferences for mobile advertising IDs
4. Visit industry-provided or proprietary opt-outs
5. "Do Not Track"

"Keeping Up with the Online Advertising Industry"

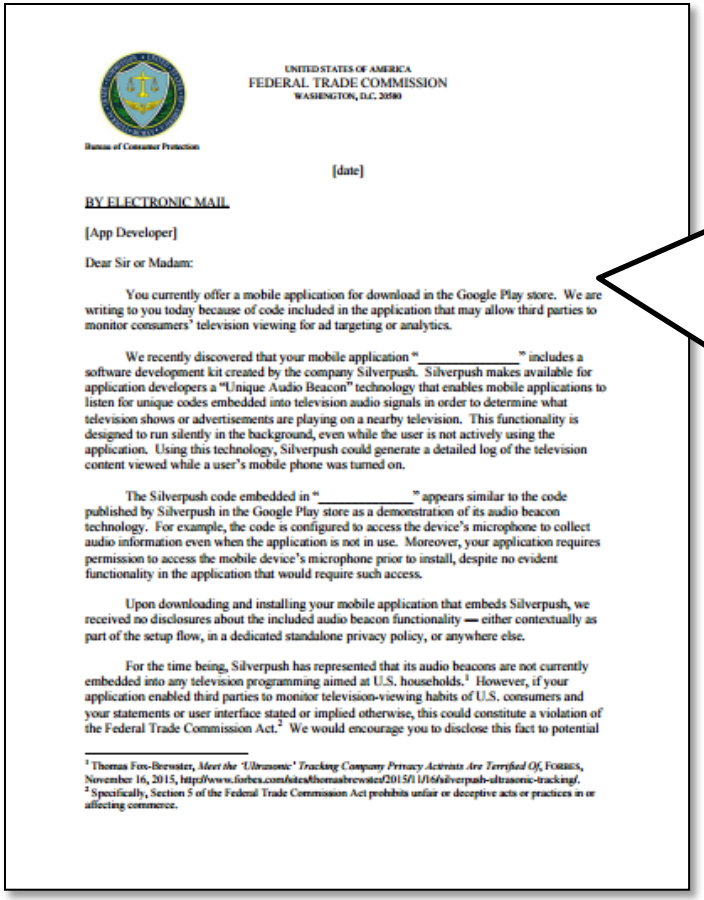
Jessica Rich, Director of the FTC Bureau of Consumer Protection, has recently emphasized that companies and self-regulatory groups must keep pace with evolving technologies

- "**Tell people how they're being tracked and offer them easy-to-use tools to block *all* of the techniques used to track them.** Industry has moved well beyond cookie-based tracking, and the choices offered to people must keep pace with what's happening in the marketplace."
- ". . . **disclosures and choices companies offer to people must address the *many* forms of tracking companies are using**, including proprietary techniques that combine technologies like cookies, fingerprinting, cookie syncing, and many others."
- "If you're collecting persistent identifiers, **be careful about making blanket statements to people assuring them that you don't collect any personal information or that the data you collect is anonymous**. And as you assess the risks to the data you collect, consider all your data, not just the data associated with a person's name or email address."

FTC Workshop on Cross-Device Tracking

- **The FTC held a workshop in November 2015 to examine key privacy and security issues raised by tracking users across their various devices, such as smartphones, tablets, desktops, TVs and other Internet-connected devices**
- **Key Issues:**
  - Transparency
  - Choice
  - Data minimization and security
- **Key takeaway**: Provide clear and conspicuous notice and choice, in a manner consistent with existing FTC and self-regulatory frameworks, and follow through with your privacy promises

Silverpush: FTC Issues Warning Letters to App Developers Using Audio Beacon Technology



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Bureau of Consumer Protection

[date]

BY ELECTRONIC MAIL

[App Developer]

Dear Sir or Madam:

You currently offer a mobile application for download in the Google Play store. We are writing to you today because of code included in the application that may allow third parties to monitor consumers' television viewing for ad targeting or analytics.

We recently discovered that your mobile application "_____" includes a software development kit created by the company Silverpush. Silverpush makes available for application developers a "Unique Audio Beacon" technology that enables mobile applications to listen for unique codes embedded into television audio signals in order to determine what television shows or advertisements are playing on a nearby television. This functionality is designed to run silently in the background, even while the user is not actively using the application. Using this technology, Silverpush could generate a detailed log of the television content viewed while a user's mobile phone was turned on.

The Silverpush code embedded in "_____" appears similar to the code published by Silverpush in the Google Play store as a demonstration of its audio beacon technology. For example, the code is configured to access the device's microphone to collect audio information even when the application is not in use. Moreover, your application requires permission to access the mobile device's microphone prior to install, despite no evident functionality in the application that would require such access.

Upon downloading and installing your mobile application that embeds Silverpush, we received no disclosures about the included audio beacon functionality — either contextually as part of the setup flow, in a dedicated standalone privacy policy, or anywhere else.

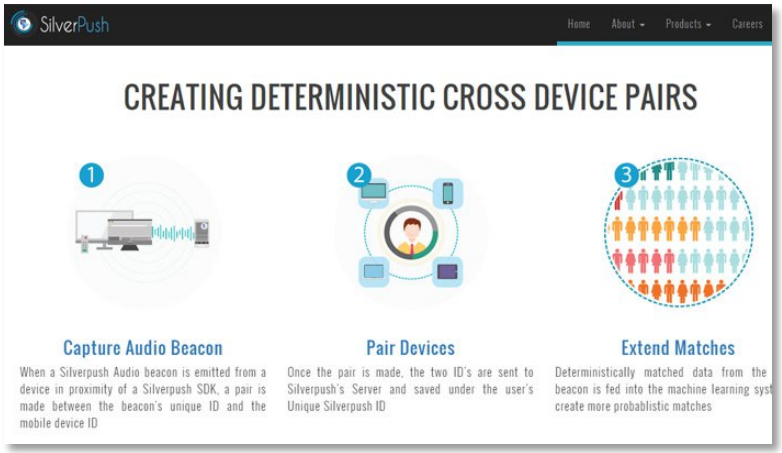
For the time being, Silverpush has represented that its audio beacons are not currently embedded into any television programming aimed at U.S. households.[1] However, if your application enabled third parties to monitor television-viewing habits of U.S. consumers and your statements or user interface stated or implied otherwise, this could constitute a violation of the Federal Trade Commission Act.[2] We would encourage you to disclose this fact to potential

[1] Thomas Fox-Brewster, *Meet the 'Ultrasonic' Tracking Company Privacy Activists Are Terrified Of*, FORBES, November 16, 2015, http://www.forbes.com/sites/thomasbrewster/2015/11/16/silverpush-ultrasonic-tracking/.
[2] Specifically, Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices in or affecting commerce.

Dear Sir or Madam: You currently offer a mobile application for download in the Google Play store. We are writing to you today because of **code included in the application that may allow third parties to monitor consumers' television viewing for ad targeting or analytics**.

Silverpush: FTC Issues Warning Letters to App Developers Using Audio Beacon Technology

- **In March 2016, the FTC issued warning letters to mobile app developers that had integrated Silverpush's "unique audio beacon" technology**
  - Third-party SDK enabled mobile applications to "listen for unique codes embedded into television audio signals in order to determine what television shows or advertisements are playing on a nearby television"
  - Code allegedly was configured to access the device's microphone even when the application is not in use
  - FTC warned app developers they must disclose this functionality and let consumers make informed choices; allegedly there were "no disclosures about the included audio beacon functionality — either contextually as part of the setup flow, in a dedicated standalone privacy policy, or anywhere else"



Self-Regulatory Guidance and Enforcement

The FTC continues to express support for self-regulation of online advertising, and self-regulatory standards track the FTC's rules and enforcement priorities

- **In November 2015, the Digital Advertising Alliance (DAA) released its long-awaited cross-device guidance**
  - Transparency—must disclose cross-device practices in privacy policy and through enhanced notice on websites or in-app
  - Control—cannot use "multi-site" or "cross-app" data from opted-out device on other devices, or vice versa, and no sharing data from that device with third parties
- **In May 2016, the Better Business Bureau's Accountability Program announced its first-ever enforcement actions against mobile app developers**
  - Failed to provide enhanced notice and choice for third-party collection of behavioral and precise location data for targeted advertising
  - Child-directed mobile apps allowed third-party collection of persistent identifiers

Mobile Privacy

FTC Enforcement of Mobile Privacy

The FTC has brought numerous cases against mobile app companies for allegedly violating promises made to consumers about their data

- **Path (2013)**: Automatically collected information from users' mobile device address books regardless of each user's selection, as well as collecting information from children
- **Brightest Flashlight (2014)**: Mobile flashlight app failed to disclose that the app transmitted users' precise location and unique device identifier to third parties, including advertising networks, and provided false option to decline sharing
- **Snapchat (2014)**: Misrepresented "ephemeral" nature of "snaps"—snaps could be preserved with third-party apps and undetected screenshots, or saved on recipients' devices—and collected users' precise location and contacts without adequate notice or consent
- **Nomi (2015)**: Retail mobile location-tracking service failed to provide in-store notice and opt-out, despite statement in privacy policy that it would "[a]lways allow consumers to opt out of Nomi's service on its website as well as at any retailer using Nomi's technology."

InMobi: FTC Alleges Mobile Advertising Network Tracked Users' Location without Permission

In June 2016, InMobi settled charges with the FTC for allegedly using WiFi network information to infer location and serve geo-targeted ads without consent, bypassing mobile platform settings that restricted access to location data

- FTC alleged that "InMobi tracked the locations of hundreds of millions of consumers, including children, without their consent, in many cases totally ignoring consumers' express privacy preferences"
- InMobi's marketing materials stated that it would collect location data only "in the form of user opt-in lat/long signals"
- InMobi also allegedly collected information from children without verifiable parental consent—despite having an option during the registration process through which app developers could indicate that the apps were directed to children
- **Key Takeaway**: FTC enforcing third-party ad platform compliance with app permissions and device privacy settings; ensure that you do not collect personal information through apps that you know (or should know) are directed to children

Vulcun: FTC Brings Enforcement Action for Force-Installing Apps and Collecting Device Info

In February 2016, Vulcun settled charges with the FTC for unfairly replacing web browser game with a program that force-installed apps onto users' mobile devices, enabling apps to access users' contacts, photos, location, and persistent identifiers

- Vulcun allegedly "commandeer[ed] people's computers, and bombard[ed] them with ads," bypassing privacy permissions and disrupting users' experiences on mobile devices and desktop computers
- Vulcun's program, *Weekly Android Apps*, allegedly hid and accepted the default Android permissions request, automatically approving default Android permissions for each force-installed app without the user's knowledge
- Force-installed apps allegedly gained immediate access to wide range of user information, and "could have gained access to other information, including financial and health information, by executing additional malicious code on the consumer's mobile device"
- **Key Takeaway**: FTC investigating efforts to bypass privacy settings and gain unauthorized access to sensitive information

Sensitive Health and Children's Information

FTC Enforcement Actions: Health Info

In December 2014, the FTC settled charges with Payments MD for allegedly violating consumers' privacy by collecting personal medical information from pharmacies, medical labs, and insurance companies, without consumers' informed consent

- "Consumers' health information is as sensitive as it gets. Using deceptive tactics to gain consumers' 'permission' to collect their full health history is contrary to the most basic privacy principles"
- Online medical bill-payment service allegedly used deceptive registration process to trick consumers into granting permission for the company and its partners to collect detailed medical information, including prescriptions, procedures, medical diagnoses, lab test results, and more
- At no point in the patient portal registration process did Payments MD notify consumers it would seek their sensitive health information from third parties for use in a fee-based "Patient Health Report" service; instead, registrants were prompted to accept four authorizations with just one click
- **Key Takeaway**: FTC requires affirmative, informed and express consent from consumers prior to collecting sensitive health information from third parties

FTC Enforcement Actions: Health Info

In June 2016, FTC settled charges with Practice Fusion for misleading consumers by soliciting and publicly posting doctor reviews containing patients' sensitive personal and medical information, without adequate disclosure and affirmative consent

- Electronic health record company allegedly sought doctor reviews for public-facing healthcare provider directory by sending emails that "appeared to be sent on behalf of patients' doctors, and ask[ing] consumers to rate their provider '[t]o help improve your service in the future'"
- Practice Fusion's emails allegedly were misleading and the privacy policy did not disclose that Practice Fusion would post the reviews
- FTC required Practice Fusion to provide clear and conspicuous notice by disclosure—separate and apart from the privacy policy, terms of use or similar document—that it was making such information publicly available, and to obtain consumers' affirmative consent prior to posting sensitive health information
- **Key Takeaway**: "Companies that collect personal health information must be clear about how they will use it – especially before posting such information publicly on the Internet."

Mobile Health App Developers: FTC Best Practices

In April 2016, the FTC released guidance for mobile health app developers. Key takeaways:

1. **Express affirmative consent**
   - Must have users' affirmative consent to collect or share health data, such as dietary info or blood pressure reading
2. **"Just in time" notice**
   - Tell users about sensitive or unexpected data the app collects, both at time of app install and time of data collection
3. **Data minimization**
   - Collect only what you need, store in de-identified form, delete after no more business need
   - Limit access and permissions and use privacy-default settings
4. **Security by design**
   - Implement security at every stage of app lifecycle
5. **Determine which federal laws apply**

FTC Actions on Children's Information

- **FTC's revised COPPA Rule includes persistent identifiers in the definition of "personal information"—and makes clear that persistent IDs cannot be used for behavioral advertising on child-directed sites or services without parental notice and consent**
- **On December 17, 2015, the FTC announced its first settlements and civil penalties against two app developers for allegedly sharing persistent IDs:**

  - **LAI Systems, LLC**, created a number of child-directed apps that allegedly permitted third-party advertisers to collect persistent identifiers without parental notice or consent

  - **Retro Dreamer** also created child-directed apps that allegedly allowed third-party advertisers to collect persistent identifiers—one ad network specifically warned Retro Dreamer over the course of 2013 and 2014
  - Civil penalties: $60K for LAI Systems and $300K for Retro Dreamer
- **In November 2015, FTC approved Riyo, Inc.'s "face match to verified photo identification" process for parental consent**

Internet of Things, Big Data, and the Fair Credit Reporting Act

FTC Comment on Internet of Things

In June 2016, the FTC filed a comment to the Department of Commerce's National Telecommunications and Information Administration (NTIA) on the benefits, challenges and role of government in fostering innovation for the rapidly growing number of devices connected to the Internet

- **Key consideration for companies: Are we collecting and using data consistent with consumer expectations, based on the context of the interaction?**
  - Unexpected collection requires consumer consent
  - Unexpected uses require clear and conspicuous notice and choice
  - Ensure downstream privacy and data protections
- **Meaningful Notice and Choice**
  - Give consumers choice for third-party sharing with data brokers or ad networks, if sharing is inconsistent with context of consumer's relationship with the manufacturer
  - Explore new ways to provide consumer choice, despite lack of traditional interface: video tutorials, QR codes on devices, choice at point of sale, set-up wizards, privacy dashboards

FTC Comment on Internet of Things (cont'd)

- **Data Minimization**
  - Seek consumer consent before collecting unexpected categories of data
- **Data Security**
  - Must ensure downstream privacy and data protections through vendor contracts and oversight
  - Monitor and patch product vulnerabilities over lifecycle
  - Failure to implement reasonable security could be deceptive or unfair practice under Section 5 of the FTC Act
- **Role for Future Regulation?**
  - FTC supports legislation to require companies to notify consumers of security breach

Enforcement Priorities for Internet of Things

- **2015 FTC Staff Report on the Internet of Things**
  - Privacy by design: Implement reasonable security and data minimization
  - Notice and choice for unexpected data collection
- **FTC Enforcement Actions**
  - **ASUSTeK**: Settled charges that router security flaws and "insecure 'cloud' services" compromised consumers' connected devices
  - **TRENDnet**: Settled charges that TRENDnet's home cameras had a vulnerability that enabled others to view and listen to camera footage
- **Key takeaway**: Put reasonable security measures in place to protect consumers' information from unauthorized disclosure through connected devices
  - Factor in the amount and sensitivity of data collected

FTC Big Data Report: January 2016

1. **Existing consumer protection and equal opportunity laws apply to big data**
   - **Fair Credit Reporting Act (FCRA)**
     - Be mindful of collecting/using/sharing analytics information for eligibility determinations
     - Even if identifying information about specific consumers is stripped away, resulting reports may still be "consumer reports" under FCRA
   - **Equal Opportunity Laws**
     - Review algorithms for hidden biases with unintended or disparate impact
     - Beware of "neutral" policies that disproportionately impact protected classes under ECOA, Title VII of the Civil Rights Act, ADA, Fair Housing Act, etc.
   - **Section 5 of the FTC Act**
     - Implement privacy by design
     - Honor promises and maintain reasonable security
2. **Beware sale of big data and fraud: FTC on high alert for fraudsters using sensitive data purchased from data brokers to harm consumers**

Fair Credit Reporting Act: Obligations

- **FCRA aims to ensure information provided by consumer reporting agencies (CRAs) is accurate**
- **In 2012, FTC issued warning letters to mobile app developers regarding the FCRA**
  - Mobile apps that assemble or evaluate consumer information—such as background reports used for employment, housing, insurance, or credit determinations—may qualify as CRAs
- **Among other things, CRAs must:**
  - Take reasonable steps to ensure report users have "permissible purpose"
  - Take reasonable steps to ensure maximum possible accuracy of report info
  - Inform report users of obligations under FCRA

Fair Credit Reporting Act Enforcement

- **Sprint Corporation (Oct. 21, 2015)**
  - $2.95M civil penalty for failure to give proper notice to low credit consumers who were charged a separate monthly fee, in violation of Risk-Based Pricing Rule
  - Risk-Based Pricing Rule: requires disclosure to help consumers understand their credit reports and alert them to possible errors
- **Tricolor Auto Acceptance, LLC (Sept. 17, 2015)**
  - $82k civil penalty for lack of policies and procedures to ensure accuracy of information reported to CRAs, in violation of FCRA's Furnisher Rule
  - Furnisher Rule: when reporting to CRAs, must have policies and procedures to ensure information is accurate and enable consumers to dispute inaccurate information with the reporting company (not the CRAs)

Enforcement of International Frameworks

International Framework Enforcement

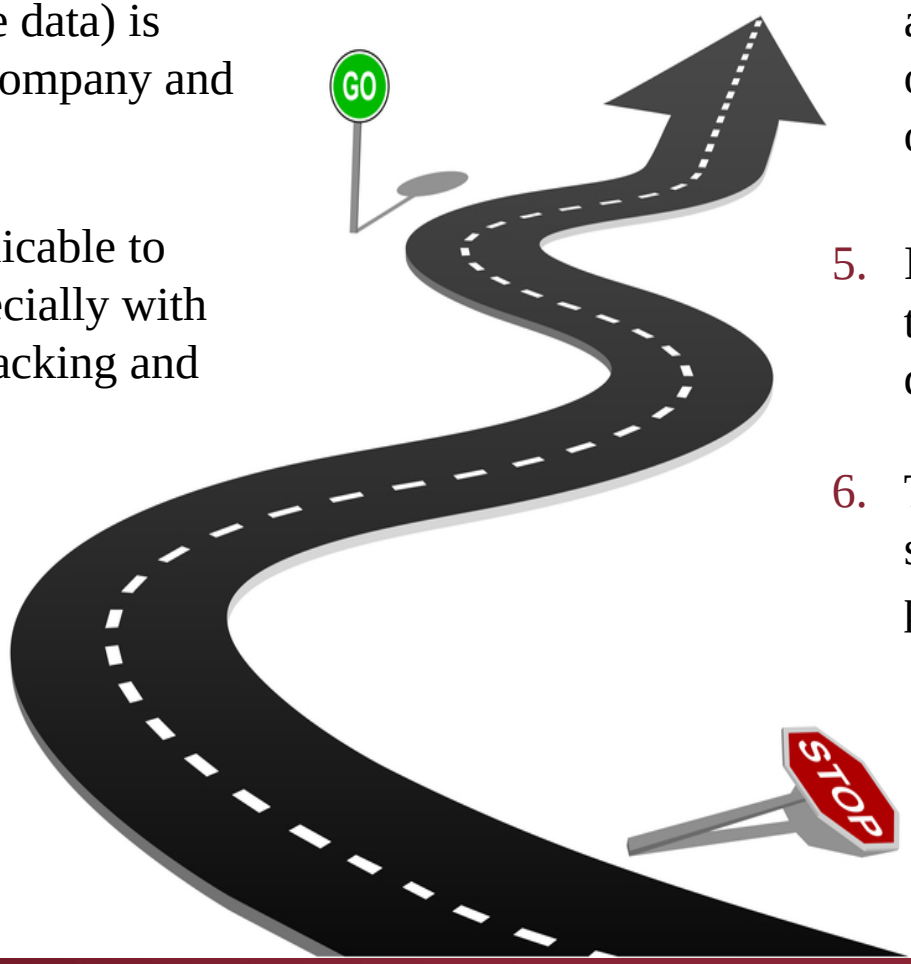
- **FTC continues to enforce companies' promises to comply with international privacy frameworks, even after the invalidation of U.S.-EU Safe Harbor**
  - Settlements in 2015 with 15 companies whose websites allegedly misled consumers by claiming to be certified members of the U.S.-EU or U.S.-Swiss Safe Harbor Frameworks
  - Companies either never certified or certifications had lapsed
- **FTC enforces Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System in the U.S.**
  - Need review by APEC-recognized accountability agent
  - Very Incognito Technologies: website falsely certified CBPR participation, but had never been certified
- **Key Takeaway**: Do not misrepresent involvement in any government or self-regulatory privacy program; keep certifications current

Roadmap for Avoiding FTC Privacy Enforcement

1. Understand what data (including sensitive data) is collected by your company and by third parties

2. Research laws applicable to your business, especially with respect to online tracking and Big Data

3. Disclose practices in a clear and conspicuous manner and ensure that privacy promises are accurate



4. Provide "enhanced notice" and choice, as appropriate, for certain online tracking and out-of-context disclosures

5. Invest in privacy throughout the product development lifecycle

6. Take reasonable steps to select and retain service providers

7. Adjust privacy program in light of changes to business

Questions?

Reed Freeman, Partner and Co-Chair Cybersecurity, Privacy and Communications Practice
+1 202 663 6267
reed.freeman@wilmerhale.com

Patrick Bernhardt, Associate
+ 1 202 663-6549
patrick.bernhardt@wilmerhale.com

Elizabeth D'Aunno, Associate
+1 202 663 6448
elizabeth.daunno@wilmerhale.com

**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 of this program also may be able to claim England & Wales Unaccredited CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.*