WilmerHale Cybersecurity, Privacy and Communications Webinar: FTC Privacy and Data Security—A Look Back and a Look Ahead

March 22, 2018

Reed Freeman, Partner

Reed Abrahamson, Senior Associate

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Attorney Advertising

Speakers

Reed Freeman
Partner

Co-Chair, Cybersecurity, Privacy, and Communications Practice Group

Reed Abrahamson
Senior Associate

Cybersecurity, Privacy, and Communications Practice Group

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 CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales 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.*

Table of Contents

New Commissioners (Coming Soon)

New Commission Members

- Four nominees unanimously approved by the Senate Commerce Committee on February 28. No full Senate confirmation vote with scheduled yet.
  - Press reports suggest delay may be related to a push by Democrats for a fifth (and Democrat) nominee.
  - FTC Chair:
    - Joseph Simons (Republican, to replace current Commissioner Terrell McSweeney (Democrat))
  - Commissioners
    - Noah Phillips (Republican, to take open seat)
    - Christine Wilson (Republican, to replace Acting Chairman Maureen Ohlhausen)
    - Rohit Chopra (Democrat, to take open seat)
- Result – Entirely new set of commissioners. If no fifth nominee is forthcoming, the four member FTC Commission would have three Republicans, one Democrat, and one open Democrat seat.

Brief Biographies

- **Joseph Simons (Republican)**
  - Co-chair of antitrust group at Paul Weiss
  - Former director of FTC Competition Bureau (2001-2003)
  - Co-developer of “critical loss analysis” technique for market definition, now part of FTC and DOJ merger guidelines

- **Christine Wilson (Republican)**
  - Senior V.P. for Regulatory & International Affairs at Delta Air Lines
  - Former partner, Kirkland & Ellis
  - Former chief of staff to former FTC Chairman Tim Muris

Brief Biographies

- **Noah Phillips (Republican)**
  - Chief counsel for Senate Majority Whip John Cornyn (since 2011)
  - Former associate at Steptoe & Johnson; Carvath Swaine & Moore
  - Clerked for Judge Prado (5th Circuit)

- **Rohit Chopra (Democrat)**
  - Senior Fellow at Consumer Federation of America
  - Former Assistant Director of CFPB (2010-2015)
  - Former associate at McKinsey & Company

Privacy Enforcement Actions

In the Matter of VIZIO, Inc. and VIZIO Inscape Services, LLC

February 6, 2017

- **Background:** VIZIO makes smart TVs, and VIZIO Inscape Services, a wholly owned subsidiary of VIZIO, makes automated content recognition (ACR) software that detects the content being displayed on smart TVs.

- **Allegations**
  - The FTC, NJ Attorney General, and NJ Department of Consumer Affairs alleged that VIZIO used ACR to track consumers' viewing habits and provided this to third parties—sometimes along with consumers' IP and MAC addresses and Wi-Fi access points. The data were used to deliver ads and track their effectiveness.
  - VIZIO allegedly did not provide notice of its use of ACR until *after* the investigation began.
  - The FTC brought an unfairness claim based on tracking and two deception counts in federal court.

In the Matter of VIZIO: Settlement

- **Rare Monetary Settlement:** VIZIO agreed to pay $1.5 million to the FTC and $1 million (with $300,000 suspended), along with reimbursement for fees and costs, to NJ.
- **Injunctive Relief**
  - VIZIO must delete data it collected before it provided notice.
  - VIZIO must also implement a comprehensive privacy program, submit to privacy assessments for 20 years, and engage in standard compliance reporting and record-keeping.
  - VIZIO must obtain consumers' consent via a prominent and easy-to-understand notice before it can obtain television viewing data.
- **Key Takeaways**
  - For the first time, the FTC treated television viewing data as "sensitive" data that, when shared without consent, "causes or is likely to cause substantial injury to a consumer."
    - TV viewing data is in the same category as health data, financial data, SSNs, precise geolocation data, and data regarding children.

In the Matter of Turn, Inc.

April 21, 2017

- **Background:** Turn uses web beacons and cookies to track consumers on their computers for targeted advertising. It also uses mobile device advertising IDs to track consumers on their mobile devices. Turn was contractually prohibited by companies like Apple and Google from correlating mobile device IDs with other identifiers. Otherwise, consumers who tried to opt out of tracking based on their mobile device IDs could still be tracked.

- **Allegations:** The FTC alleged that Turn synced mobile device ad IDs with tracking identifiers created by Verizon Wireless, allowing it to keep state on users even after they deleted cookies or reset their mobile device ad IDs. Turn was also allegedly able to respawn deleted cookies.

- **Settlement:** The FTC and Turn reached a settlement in which Turn is required avoid misrepresentations; create a clear and conspicuous opt-out mechanism and prominently display it on its website; honor opt-out signals; and engage in certain compliance, reporting, and recordkeeping activities.

Decusoft, LLC; Tru Communications, LLC; Md7, LLC

September 8, 2017

- **Background:** Decusoft develops HR software, Tru Communications provides printing services, and Md7 “assists wireless operators in managing real estate-related issues.”

- **Allegations:** The FTC alleged that the three companies represented that they were certified under the EU-U.S. Privacy Shield and that Decusoft falsely represented it was certified under the Swiss-U.S. Privacy Shield. In reality, according to the FTC, they never completed the certification processes to participate in these programs.

- **Settlement:** The companies are prohibited from misrepresenting their participation in privacy programs and must comply with certain compliance and reporting requirements for twenty years.

- **Similar Case:** Sentinel Labs, Inc.; SpyChatter, Inc.; and Vir2us, Inc. alleged to have falsely stated that they complied with the APEC Cross-Border Privacy Rules system (CBPR).

VTech Electronics

January 8, 2018

- **Background:** VTech Electronics makes connected electronic toys that used its "Kid Connect App" and its "Learning Lodge Navigator" online platform. The app and online platform required the creation of user accounts by parents on behalf of children.

- **Allegations:** The FTC alleged that the process for creating children's accounts was not compliant with COPPA and the FTC's COPPA Rule and that millions of accounts were created for children, who could then provide their personal information, without providing COPPA compliant direct notice to parents and obtaining "verifiable parental consent." The FTC also alleged that VTech made statements about account data encryption that were untrue.

- **Settlement:** The FTC imposed a $650,000 civil penalty. VTech is enjoined from further COPPA violations. VTech may not make other misrepresentations, must establish a comprehensive information security program, and must engage in compliance assessments and reporting for 20 years.

Prime Sites, Inc. d/b/a Explore Talent

February 5, 2018

- **Background:** Explore Talent operates an online service for actors, models, and other artists, providing information about "auditions, casting calls, and other professional opportunities." The sign up process did not screen users who indicated they were under age 13.
- **Allegations:** The FTC alleged that over 100,000 Explore Talent members were under age 13, and Explore Talent had not taken steps to obtain verifiable parental consent or prevent users under the age of 13 from signing up. The FTC also alleged that Explore Talent falsely told users they needed to sign up for paid memberships to access specific job opportunities.
- **Settlement:** The FTC imposed a $500,000 civil penalty (of which the company will pay $235,000, with the reminder suspended). Information collected in violation of COPPA must be deleted. Explore Talent may not make other misrepresentations and must engage in compliance reporting for 20 years.

In re PayPal, Inc. (The Venmo Case)

February 27, 2018

- **Background:** PayPal operates Venmo, an application that allows for peer-to-peer payments. By default, Venmo made each user's last five public transactions visible on each user's Venmo webpage, which was accessible by the public. Fully disabling this display required adjusting two different privacy settings.
- **Section 5 Privacy Allegations:** The FTC alleged that Venmo:
  - Made affirmative misrepresentations about the process for disabling public display of a user's transaction history when it described only one of the two settings that had to be adjusted to keep the transaction private; and
  - Failed to inform users that, unless the second setting was also adjusted, another user could make the transaction public.
- **Section 5 Security Allegations:** The FTC alleged that Venmo:
  - Mispresented the security safeguards it had in place to protect the security, confidentiality, and integrity of consumer information. Venmo claimed to have implemented "bank-grade security systems and data encryption."
  - FTC argued these statements were not true because Venmo failed to implement "sufficient safeguards" (like automatic security notifications) which left consumer accounts vulnerable to take over and misuse, which had occurred in some cases.

In re PayPal, Inc. (The Venmo Case)

- **GLBA Allegations:** The FTC alleged that Venmo was a financial institution engaged in "transferring money," and required to comply with the GLBA.
  - **Privacy Allegations:** The FTC alleged that:
    - Venmo's in-app privacy notice was not presented clearly and conspicuously, because the link to the privacy policy was in "grey text on a light grey background."
    - The privacy notice was misleading (same conduct as lead to the Section 5 allegations).
    - Venmo had not delivered the privacy notice in a way that was reasonably calculated to ensure that customers received it, because the notice was made available only through a link in the application and customers were not required to acknowledge receipt.
  - **Safeguards Allegations:** The FTC also alleged that, for a period of time, Venmo had no written information security program, had not conducted a required risk assessment, and had not implemented basic security safeguards for accounts.

In re PayPal, Inc. (The Venmo Case)

- **Settlement:**
  - Further misrepresentations are prohibited.
  - Venmo must provide users with a supplementary privacy disclosure describing the process required to make all transaction records private. The disclosure cannot contain any other information.
  - Venmo may not violate the GLBA's privacy regulations (Regulation P, 12 C.F.R. Part 1016) or safeguards regulations (16 C.F.R. Part 314).
  - An initial assessment, followed by assessments every two years for ten years to confirm:
    - compliance with the administrative, technical, and physical safeguards Venmo has implemented.
    - that the safeguards implemented are appropriate for Venmo's size, complexity, activities, and sensitive customer information.
    - that the safeguards implemented are consistent with the requirements of 16 C.F.R. Part 314.
    - that the security program is sufficient to protect the confidentiality, security, and integrity of Venmo customer's confidential information.

Data Security Enforcement Actions

In the Matter of D-Link and D-Link Systems, Inc.

No. 3:17-cv-00039, 2017 WL 4150873, (N.D. Cal. Sept. 19, 2017).

- **Background:** D-Link and its U.S. subsidiary manufacture networked devices such as routers and IP cameras.
- **Allegations:** The FTC brought an unfairness claim and deception claims relating to various devices and the companies' public statements about data security:
  - D-Link "failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access."
  - D-Link misrepresented to consumers that products were safe. D-Link asserted that the devices were "easy to secure" and that its router was "one of the safest."
- **Court's Opinion:** The FTC's complaint did not allege that consumers ever *actually* suffered harm from using D-Link's products; it alleged only that "[c]onsumers are likely to suffer substantial injury"—a theory of harm similar to the one that the 11th Circuit said may have been lacking in *Lab MD v. FTC,* 678 F. App'x 816 (11th Cir. 2016). The district court dismissed the unfairness claim because it found the FTC failed to allege anything more than "a mere possibility of injury at best." The deception claims also dismissed for failure to identify misleading statements.

In the Matter of TaxSlayer, LLC

August 29, 2017

- **Background:** TaxSlayer promotes an online and app-based service to assist consumers in filling out their tax returns.
- **Allegations Regarding the Privacy Rule and Regulation P:** The FTC alleged that TaxSlayer's required privacy notice, located at the end of a licensing agreement, was not clear and conspicuous, and not delivered in a way that could be expected to result in actual notice because consumers were not required to acknowledge receipt before using TaxSlayer's services.
- **Allegations Regarding the Safeguards Rule:** The FTC alleged that TaxSlayer failed to comply with the Safeguards Rule because it failed to establish an information security program; conduct risk assessments; and implement appropriate account authentication and protection safeguards.
  - FTC alleged that hackers gained access to thousands of accounts and committed identity theft.
- **Settlement:** TaxSlayer enjoined from violating Regulation P and the Safeguards Rule; must obtain biennial privacy and data security assessments from a third party for 10 years explaining how TaxSlayer is complying with the Safeguards Rule; and must engage in certain compliance, reporting, and record-keeping activities.

Initiatives

Economics of Privacy Initiative

- In early 2017, Acting Chairwoman Maureen Ohlhausen announced that the FTC would seek to deepen its "understanding of the economics of privacy," including by "studying consumer preferences and the relationship between access to consumer information and innovation."
- The FTC held a December 12, 2017 workshop on Information Injury. The panels included:
  - Injuries 101 (the types of injuries that can result from unauthorized access or misuse of information).
  - Potential Factors in Assessing Injury.
  - Business and Consumer Perspectives (the benefits and costs of information collection and sharing from different perspectives).
  - Measuring Injury (how to quantify injury and the risk of injury and how to incorporate consumers' preferences).

Children's Online Privacy Protection Act (COPPA)

- Among other things, COPPA requires operators of websites directed at children, and operators of websites with actual knowledge that they are collection children's personal information, to give notice to parents and obtain consent.
  - PI includes, among other things, photograph, video, or audio files.
- On October 20, 2017, the FTC released an Enforcement Policy Statement on COPPA and voice recordings collected as part of speech-to-text functionality.
  - The FTC stated that gathering such data constitutes "collection" under COPPA, even if it is very quickly deleted.
  - However, in general, "when a covered operator collects an audio file containing a child's voice solely as a replacement for written words . . ., but only maintains the file for the brief time necessary for that purpose, the FTC would not take an enforcement action against the operator" as long as it provides notice as required by COPPA.
- In addition, the FTC has published a COPPA compliance plan to help businesses comply with the law.

Stick With Security Blog Series

- In 2017, the FTC published the *Stick With Security* series of blog posts, which offers additional insight into the ten principles in its *Start With Security* guidance.
- The blog posts are based off of recent law enforcement actions, closed investigations, and companies' experiences.
- The posts emphasize, among other things, that companies should:
  - Not collect data, use, or retain data unnecessarily.
  - Impose sensible data access restrictions and controls.
  - Require secure passwords.
  - Securely store and transmit personal information.
  - Segment and monitor network.
  - Secure any remote access to networks.
  - Maintain sound security when developing a new product.
  - Make service providers implement reasonable security.
  - Implement procedures to keep security current and address any vulnerabilities.
  - Physically secure devices, physical media, and paper.

Connected Cars Workshop (FTC and NHTSA)

June 28, 2017

- According to experts, risks of connected cars include, among others:
  - Increasing connectedness means more potential vulnerabilities, and these should be addressed.
  - The sorts of data collected by connected cars may be sensitive (e.g., biometric data, geolocation data). Privacy advocates worried about the ability of companies to protect and properly use these data.
- Ohlhausen said that the FTC's approach is one of "regulatory humility" and that regulators should avoid hindering development.
  - But she noted that the FTC could take action against manufacturers and service providers in appropriate circumstances.
- Terry Shelton, Acting Director of NHTSA, emphasized the role of the private sector in developing safety features and standards but said that government must enforce consumer protection standards.
- Acting Director Tom Pahl alluded to the need for communication between government, cybersecurity experts, trade associations, and other stakeholders in crafting thoughtful guidance and self-imposed industry standards.
- Participants lauded industry efforts at collaboration and self-regulation.
- The FTC issued a brief Staff Perspective on the workshop on January 9, 2018, summarizing key themes from the day. The webpage for the workshop is here.

Speeches and Reports

Cross-Device Tracking Report

January 23, 2017

- Cross-device tracking allows companies to link multiple devices with the same person, which allows for robust tracking and targeted ads and services.
  - Deterministic: user account.
  - Probabilistic: IP addresses and geolocation information.
- Privacy and security concerns
- Self-Regulation
  - The FTC “commends” efforts by the NAI and DAA but maintains that these efforts could be ‘”strengthen[ed].”
- The FTC’s Recommendations
  - Transparency: disclose “meaningful” information to consumers.
  - Choice: the FTC suggests that device-by-device opt-outs are sufficient, for now.
  - Sensitive Data: provide heightened levels of protection.
  - Security: maintain reasonable security.
- The DAA has also issued guidance on cross-device tracking.

Ohlhuasen Keynote at ABA Consumer Protection Conference – FTC Focus Areas Under Her Leadership

February 2, 2017

Three reforms offered by Ohlhausen:

- Refocus the FTC on fraudulent schemes, especially those targeting military personnel and small businesses.
- Ensure that enforcement actions address concrete consumer injury—i.e., where consumers are actually or likely to be injured.
  - Concrete (monetary injury and unwarranted safety risks) vs. speculative or subjective injury.
  - Turning pieces of "non-sensitive consumer information into a potentially sensitive mosaic of a consumer" may require more than notice and choice.
- Reduce regulatory burdens and provide greater transparency to businesses.

Also, the FTC is seeking comprehensive data security legislation that would "give the FTC the ability to seek civil penalties to help deter unlawful conduct" - Ohlhausen Testimony on Small Business Cybersecurity (March 8, 2017)

Ohlhuasen Remarks on Informational Injury in FTC Privacy and Data Security Cases

September 19, 2017

- "Government does the most good with the fewest unintended side effects when it focuses on stopping substantial consumer injury instead of expending resources to prevent hypothetical injuries. . . . [R]egardless of the legal authority being used [deception or unfairness], the Commission . . . should always consider consumer injury in determining what cases to pursue."
- Types of injury:
  - Deception or subverting consumer choice.
  - Financial harm (including direct and indirect).
  - Health or safety.
  - Unwarranted intrusion.
  - Reputational injury (deceptiveness)

Note: Acting Chairman Ohlhausen's speeches and initiatives are hers, and the new FTC Chairman may take a different approach. This remains to be seen.

Mobile Security Updates: Understanding the Issues

February 28, 2018

- Report issued after the FTC requested information from eight mobile device manufacturers.
- The report highlights a variety of risks associated with the security update process, including consumer inactivity and devices aging out of support.
- Report calls for:
  - Increased consumer education about the update process and the importance of updates.
  - Ensuring that devices are supported and updated for a period of time consistent with consumer expectations.
  - Improved record-keeping by manufacturers around update decisions.
  - A more streamlined security update process, including “security-only” updates that are not bundled with other, general software updates.
  - Manufacturers to adopt and disclose minimum guaranteed support periods for devices, and notice to consumers when support periods are about to end.

Looking Ahead to 2018: Key Privacy Takeaways

- First, with an entirely new Commission, it's impossible to make predictions with a very high degree of confidence. Nevertheless, we think that:
  - The FTC will likely continue grappling with what constitutes "sensitive data," potentially leading to more types of data included in this category.
  - The FTC will also examine what constitutes "injury" and "substantial injury" in the context of privacy and data security cases. Must there be "concrete" harm? Is merely having information breached or exposed an injury? How should businesses evaluate tradeoffs to collecting and using information?
    - *Informational Injury Workshop*, Dec. 12, 2017.
  - Cookieless tracking and other technologies that make it easier to keep state on consumers will continue to draw the FTC's critical eye. Alleged abuses relating to geolocation information are also likely to draw scrutiny.

Looking Ahead to 2018: Key Data Security Takeaways

- The FTC will continue to ensure that companies have privacy policies that are readily accessible. And broken promises will make the FTC unhappy.
- After *LabMD* and *D-Link*, the FTC may be less likely to bring cases based on theories of intangible injury—at least until after it concludes its consideration of what constitutes "injury."
- The FTC will continue to investigate data breaches, especially those large in scale and otherwise newsworthy.
- The greatest risks posed by the FTC are likely to arise when: (1) consumers face actual injury from a data breach; and (2) the breach exposes misrepresentations with respect to data security.
- The FTC's view of "reasonable security" is opaque and fact-specific, but the FTC may be increasingly interested in encryption and stronger authentication methods. The FTC has published guidance in its *Start With Security* document which draws on lessons from the FTC's enforcement activity, and its *Stick With Security* blog posts.

Questions?

Reed Freeman
reed.freeman@wilmerhale.com
+1 202 663 6267

Reed Abrahamson
reed.abrahamson@wilmerhale.com
+1 202 663 6505

**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 CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales 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.*