WilmerHale Cybersecurity, Privacy and Communications Webinar: Hot Topics at the FTC

December 7, 2017

Reed Freeman, Partner
Sol Eppel, Associate

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Attorney Advertising

Speakers

Reed Freeman, Partner

Sol Eppel, Associate

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.*

Privacy Cases

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.
  - In addition, VIZIO allegedly failed to deliver offers and program suggestions that were promised in product literature about its "Smart Interactivity" feature.

In the Matter of VIZIO: Settlement

- The FTC brought an unfairness claim based on tracking and two deception counts in federal court.
- **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.
  - This is rare.
- **Injunctive Relief**
  - VIZIO must delete data it collected before it provided notice.
  - VIZIO must also implement a comprehensive privacy program, submit to third-party 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.

In the Matter of VIZIO: Sensitive Data

- 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."
  - So, TV viewing data is in the same category as health data, financial data, SSNs, precise geolocation data, and data regarding children.
- Although voting to approve the complaint and proposed Order, Acting Chairman Ohlhausen noted that "[t]his case demonstrates the need for the FTC to examine more rigorously what constitutes 'substantial injury' in the context of information about consumers" and indicated that she "will launch an effort to examine this important issue further."
- Note: On October 19, the President nominated Joseph Simons to chair the FTC. His confirmation hearing has not yet been set, and he has given no indication regarding the focus on "substantial injury" under his leadership.

In the Matter of Turn, Inc.

April 21, 2017

- **Background:** Turn uses web beacons and cookies to track consumers on their computers. They also use mobile device advertising IDs to track consumers on their mobile devices. These tracking data are then used for targeted advertising. 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.

In the Matter of Turn, Inc.: Settlement

- The FTC brought two counts, alleging that Turn made misrepresentations regarding users' ability to opt out of tracking mechanisms and to delete cookies.
- The FTC and Turn reached a settlement in which Turn is required to:
  - Not make any misrepresentations about the privacy of certain information.
  - Create a clear and conspicuous opt-out mechanism so consumers can opt out of targeted advertising, and prominently display it on its website.
  - Must honor opt-out signals.
  - Must engage in certain compliance, reporting, and recordkeeping activities.
- Note that the FCC brought a similar case against Verizon for allegedly inserting undeletable "supercookies" in consumers' browsers without their knowledge or consent. Verizon settled, and it must pay the FCC $1.35 million, adopt a three-year compliance plan, and provide proper notice and consent.

Sentinel Labs, Inc.; SpyChatter, Inc.; and Vir2us, Inc.
February 28, 2017

- **Background:** Sentinel Labs, Inc. provides network security software, SpyChatter, Inc. provides a private messaging app, and Vir2us, Inc. provides cybersecurity software.

- **Allegations:** According to the FTC, the companies' policies falsely stated that they complied with the APEC Cross-Border Privacy Rules system (CBPR), which allows companies to transfer data among APEC countries if they certify they meet certain standards.

- **Settlement:** The companies are prohibited from misrepresenting their participation, membership, or certification regarding any privacy or security program sponsored by a government or self-regulatory or standard-setting organization.

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.

Data Security Cases

In the Matter of D-Link and D-Link Systems, Inc.
May 22, 2017

- **Background:** D-Link and its U.S. subsidiary manufacture networked devices such as routers and IP cameras.
- **Allegations:**
  - D-Link allegedly "failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access." Specifically, it allegedly did not:
    - Take measures to protect against hard-coded user credentials and backdoors
    - Secure mobile app login credentials
    - Secure D-Link's private key—which was available on a public site for six months
  - D-Link allegedly misrepresented to consumers that products were safe.
    - For example, D-Link asserted, among other things, that the devices were "easy to secure" and that its router was "one of the safest."
  - The FTC brought an unfairness claim and 5 deception claims under Section 5 of the FTC Act relating to various devices and the companies' public statements about data security.

In the Matter of D-Link

- The FTC's complaint did not allege that consumers ever *actually* suffered harm from using D-Link's products. Instead, 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).
- In September, a court dismissed the unfairness claim because it found the FTC failed to allege anything more than "a mere possibility of injury at best." *FTC v. D-Link Systems, Inc*., No. 3:17-cv-00039, 2017 WL 4150873, at *5 (N.D. Cal. Sept. 19, 2017).
  - The Court noted that the FTC had already conducted "a thorough investigation before filing the complaint" and claimed that the "challenged security flaws" had existed for years," with no harm to be found. *Id.*
- The court also dismissed two misrepresentation claims 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. As part of this service, it collects name, SSN, contact info, employment status, income information, other information necessary to fill out a return, and IP addresses and other identifiers.

In the Matter of TaxSlayer, LLC

- **Allegations Regarding the Privacy Rule and Regulation P:**
  - The GLBA (*e.g.*, 16 C.F.R. § 313.1 et seq.) generally requires financial institutions to provide an initial and annual privacy notice that:
    - Is “clear and conspicuous.”
    - “Accurately reflects [the institution’s] privacy policies and practices.”
    - Includes specified elements, such as the information collected, the categories of third parties to whom the information is disclosed, and the security and confidentiality policies of the financial institution.
    - Additionally, according to the FTC, a financial institution must provide its privacy notice so that each consumer can reasonably be expected to receive **actual** notice.
  - The FTC alleged that TaxSlayer did not make its notice clear and conspicuous because it was at the end of a licensing agreement, and that it did not deliver the notice 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.

In the Matter of TaxSlayer, LLC

- **Allegations Regarding the Safeguards Rule:**
  - The GLBA (15 U.S.C. § 6801(b)) also requires financial institutions to implement "administrative, technical, and physical safeguards" that:
    - Ensure "the security and confidentiality of customer records and information."
    - "[P]rotect against any anticipated threats or hazards to the security or integrity of such records."
    - "[P]rotect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."
  - Implementing regulations require financial institutions regulated by the GLBA to, among other things, create and update information security programs, carry out risk assessments and mitigate any identified risks, and oversee service providers and contractually require them to protect information.

In the Matter of TaxSlayer, LLC

- **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.
    - Failed to conduct risk assessments.
    - Failed to implement appropriate authentication safeguards by not requiring consumers to create strong passwords, not informing consumers when material changes were made to their account (such as their mailing address), not validating emails upon account creation, and by allowing hackers to gain access to accounts using validation attacks.
  - As a result of these alleged violations, the FTC alleged that hackers gained access to nearly 8,900 accounts and committed identity theft with respect to some consumers by changing routing information for tax refunds to themselves.

In the Matter of TaxSlayer, LLC: Settlement

- The FTC and TaxSlayer reached a settlement, which provides that TaxSlayer:
  - Is 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.
  - 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."
- In a speech a few months later, Acting Director of the Bureau of Consumer Protection, Thomas Pahl, explained that the Bureau of Economics will be leading the initiative.
- The FTC released the agenda for December 12, 2017 workshop on Information Injury on November 28, 2017. The panels are:
  - 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 collecting children's personal information, to give notice to parents and obtain consent.
  - PI includes, among other things, photograph, video, and 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 states 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 on recent law enforcement actions, closed investigations, and companies' experiences.
- The posts emphasize, among other things, that companies should:
  - Not collect, use, or retain data unnecessarily.
  - Impose sensible data access restrictions and controls.
  - Require secure passwords.
  - Securely store and transmit personal information.
  - Segment and monitor networks.
  - 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, then-Acting Executive 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.
- Some participants lauded industry efforts at collaboration and self-regulation.
- The FTC may issue guidance or a report based on this workshop and any public comments filed.
- 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 report suggests that device-by-device opt-outs are sufficient, for now.
  - Sensitive Data: provide heightened levels of protection.
  - Security: maintain reasonable security.

Ohlhuasen Keynote at ABA Consumer Protection Conference

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.
  - Economics of Privacy Initiative.
  - 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.

Ohlhausen Testimony on Small Business Cybersecurity

March 8, 2017

- "The Commission has made clear that it does not require perfect security; that reasonable security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law."
  - "By learning about alleged lapses that led to law enforcement action, companies can improve their practices to avoid fundamental security missteps."

- "The FTC closes far more data security cases than it pursues to settlement or litigation."

- The FTC is continuing to seek "comprehensive data security legislation that would (1) strengthen its existing data security authority and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach."

Acting Director Tom Pahl's Remarks at the Public Policy Conference Law & Economics of Privacy and Data Security

May 1, 2017

- *Symbiosis between FTC approach and industry development*: "Case-by-case enforcement, paired with general research and policy statements about the thrust of FTC's enforcement actions, is well suited to addressing topics like privacy where markets and technology are so dynamic. Prescriptive rules create high risks of over-regulating and under-regulating, and proceeding case-by-case helps us avoid these types of risks."

- According to Acting Director Pahl, three areas that may have an impact on the future of privacy enforcement:
  - FTC should address broadband ISP privacy issues.
  - The FTC will continue to study novel privacy topics.
  - Economics of Privacy Initiative.

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).
- According to Ohlhausen, when deciding to bring a case, the FTC will also consider the strength of evidence linking the challenged practices to the injury; the magnitude of injury (including number of consumers); and the likelihood of injury.

Looking Ahead to 2018: Key Privacy Takeaways

- 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.
- The FTC will continue to ensure that companies have privacy policies that are readily accessible. And broken promises will be low-hanging fruit for the FTC.

Looking Ahead to 2018: Key Data Security Takeaways

- 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 risk posed by the FTC following a breach are likely to arise when: (1) consumers face actual injury; and (2) the breach exposes misrepresentations with respect to data security.
- The FTC's view of "reasonable security" is 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

Sol Eppel
sol.eppel@wilmerhale.com
+1 202 663 6914

**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.*