Cybersecurity, Privacy and Communications Webinar: Trump Administration—Updates on Cyber and Privacy Policies

January 26, 2017

Reed Freeman, Partner, WilmerHale
Jon Yarowsky, Partner, WilmerHale
Kirsten Donaldson, Counsel, WilmerHale

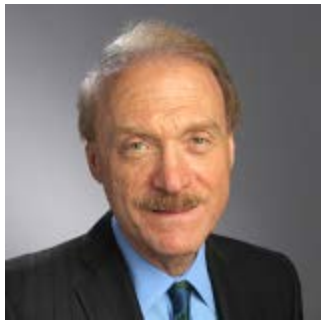
WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Attorney Advertising

Speakers

Reed Freeman
Partner



Jonathan Yarowsky
Partner

Kirsten Donaldson
Counsel

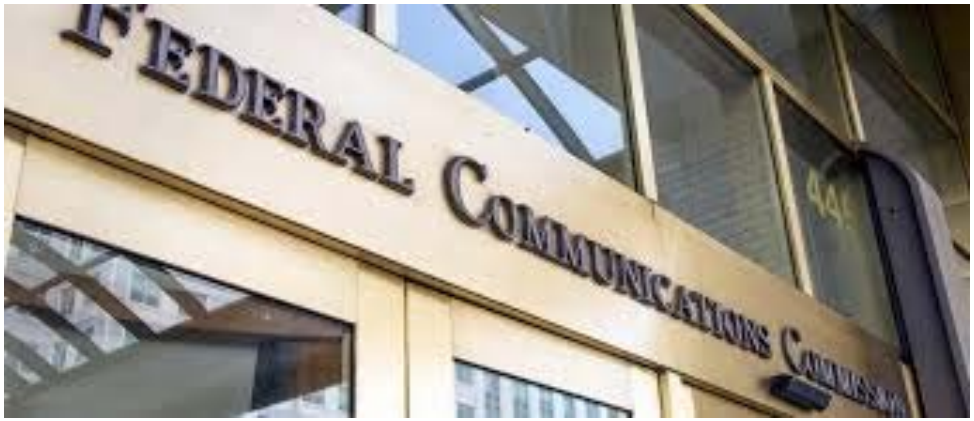
Webinar Guidelines

- 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

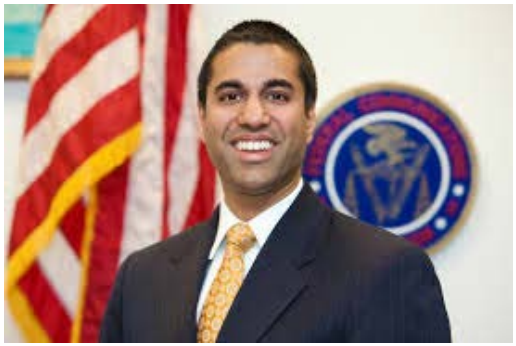
**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program will 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.*

FCC: Big Picture

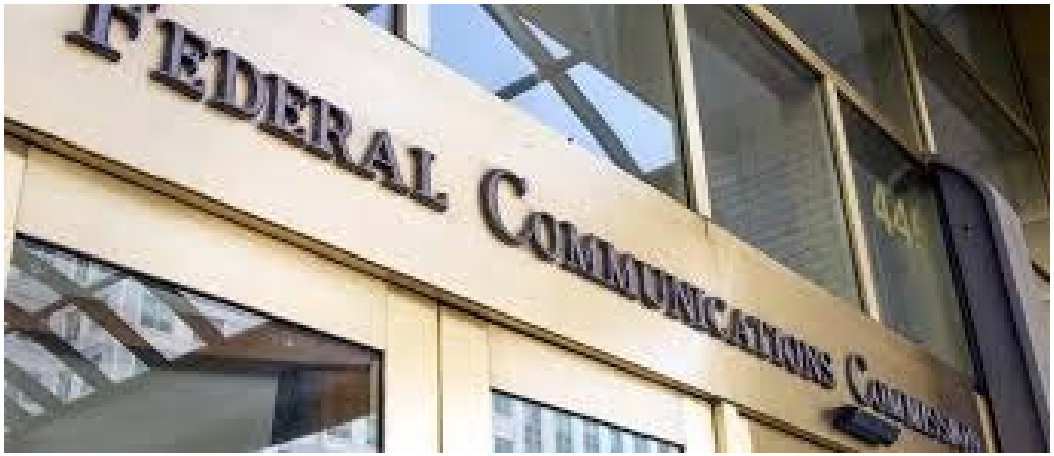
- Status of current vacancies
- Interaction with Congress (House vs. Senate)?
- A new relationship between the FCC and the FTC?
- White House role in shaping the larger mission of the FCC

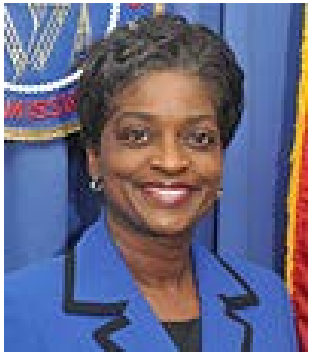


FCC: Big Picture

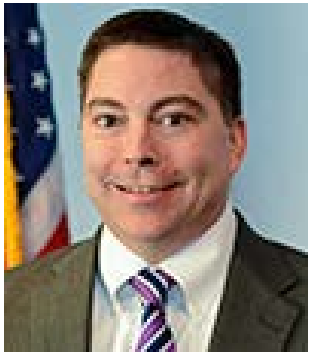


Ajit Pai (R),
Term: May 7, 2017





Mignon Clyburn (D),
Term: July 1, 2017



Michael O'Rielly (R),
Term: January 29, 2019

- 2-1 Majority
- Two Seats Yet to Fill

Net Neutrality:

Timeline:

- November 10, 2014: President Obama urged the US government to preserve "a free and open Internet."
- February 26, 2015: The FCC approved new Net neutrality rules to reclassify broadband as a Title II telecommunications service.
- June 12, 2015: Net neutrality rules went into effect.
- June 14, 2016: The FCC's rules were upheld by the U.S. Court of Appeals for the D.C. Circuit.

- Net Neutrality in a Trump Administration?

- Congressional Action?

Broadband Privacy Rule

- Opt-in: The new privacy rules require fixed and mobile ISPs to get opt-in consent from consumers before sharing Web browsing data and other private information with advertisers and other third parties.
- The FCC voted for the rules on October 27, and they partially took effect on January 3 (some rules delayed for later years).
- Opponents had 30 days to petition for reconsideration, which gave opponents until January 3 to file petitions.
- On January 3, trade groups filed petitions asking the FCC to reconsider the rulemaking.
- Normally, these petitions for reconsideration would be rejected by the FCC.
- But in this case, the privacy rules were passed 3-2 along party lines, and the two Republicans now enjoy a 2-1 majority. (Wheeler resigned and Rosenworcel's term expired).
- Possible appeal in court if the FCC eliminates the privacy rules in response to the petition for reconsideration.

“Unlock the Box”

- On February 18, 2016, the FCC proposed a new set of rules to “Unlock the box” to allow pay-TV customers who use these services to attach devices of their own choosing to their TV to watch programming without a rented box.
- No FCC statutory authority to regulate “Over The Top” providers, therefore they’re excluded in the rules.
- Stakeholder Opposition
  - Pay-TV companies and entertainment companies opposed on copyright grounds.
  - App developers also opposed an FCC committee mandating or influencing app development.
  - Letters from Congress
- September, 2016, FCC Chairman Wheeler announced an alternative proposal: Pay-TV operators would have been required to provide apps to third-party box manufacturers that mimic the functionality of their proprietary boxes. The text of this proposal was never made public.
- On September 1: Senate Commerce Committee FCC oversight hearing with Chairman Wheeler and the four Commissioners as witnesses.
- The Commissioners never reached agreement on an alternative proposal and now, with Chairman Wheeler stepping down, it is unlikely to move.

Broad Past Trends at the FTC

- The FTC's activities have, in general, enjoyed bipartisan support.
- The FTC first became concerned about online privacy in the 1990s under Democratic leadership.
- Republican Commissioners continued to focus on privacy in the 2000s.
  - Republicans brought many early online privacy cases.
  - A separate privacy division (the Division of Privacy and Identity Protection) was created during this time.
- During the Obama administration, Commissioners from both sides largely agreed on privacy and data security matters.
  - The FTC focused heavily on privacy and data security through enforcement actions, workshops, reports, and the creation of the Office of Technology Research
- That said, there have been some areas of disagreement, mostly at the margins.

Privacy: Past Administration

- The FTC took aggressive stances on privacy during the past administration.
  - *In re Nomi* (2015): The FTC alleged that Nomi helped brick-and-mortar retailers track consumer behavior using their mobile devices but did not require retailers to disclose this practice. Nomi also allowed consumers to opt out online and erroneously represented that users could opt out in stores.
- The Republican Commissioners have dissented from some of these stances.
  - Concrete vs. speculative harm.
    - *In re Nomi*: Commissioner Ohlhausen (appointed interim Chairwoman yesterday) dissented because (1) Nomi did not collect PI and thus did not have to offer an opt-out, (2) its erroneous representation did not benefit Nomi or cause tangible harm, and (3) she believed that the FTC's enforcement action would actually discourage companies from trying to go above and beyond the bare legal minimum in providing privacy protections. Commissioner Wright also dissented.
    - Internet of Things (IoT) Report: Commissioner Ohlhausen criticized the report's focus on data minimization as an unnecessary effort to prevent only hypothetical harms.
  - Cost/benefit analysis.
    - IoT Report: Commissioner Wright dissented, in part because its focus on data minimization did not consider the costs to consumers and businesses.

Privacy: Going Forward

- Under the new administration, the FTC is likely to continue to bring privacy enforcement actions based on the deception prong of Section 5 of the FTC Act (e.g., cases involving misrepresentations or material omissions regarding privacy practices).
- However, the FTC is likely to bring enforcement actions rooted in the unfairness prong of Section 5 of the FTC Act only where consumers have faced concrete injury, not intangible injury or the mere possibility of injury.
- Enforcement actions and recommendations for businesses will likely be tempered to allow businesses to innovate and will involve more cost-benefit analysis.
- There is likely to be increased skepticism of the need for, and efficacy of, new legislation.

Data Security: Past Administration

- Under President Obama, the FTC pushed the boundaries of Section 5 in data security actions.
  - *In re LabMD* (2016): The FTC alleged that LabMD inadvertently exposed consumers' personal data on a peer-to-peer file-sharing network. The FTC contended that LabMD failed to reasonably protect consumer data—even though there was no evidence that any consumer suffered any harm, such as identity theft or physical harm.
    - The FTC argued (1) that consumers suffered an intangible harm to their privacy, and (2) that the exposure of the files was likely to cause substantial injury.
    - The Eleventh Circuit has since stayed the decision, holding that the FTC's interpretation of Section 5 may well be unreasonable. *LabMD v. FTC*, No. 16-16270 (11th Cir. 2016).
- The FTC also pushed the concept of "security by design."
  - Commissioner Wright criticized the IoT Report's focus on security by design as lacking any "analytical content." Instead, he emphasized that economic cost-benefit analysis would protect consumers while more effectively cultivating innovation.

Data Security: Going Forward

- Under the new administration, the FTC is likely to bring data security actions only where consumers suffered actual, tangible harm, or faced a serious risk of such harm.
  - *Compare In re BJ's Wholesale Club* (2008): The FTC alleged that BJ's did not protect credit card and other personal information, and fraudulent purchases were made on customers' cards. The FTC argued that BJ's failed to reasonably protect consumer data.
- In deciding what to recommend with respect to data security, the FTC is likely to focus more on weighing the costs and benefits, rather than assuming that more security is always better.

Past and Future Legislative Efforts

- 150+ bills introduced in the 114th Congress to address various data protection, privacy, and cybersecurity issues, with more than a dozen receiving Committee or Floor action
- Major issues include:
  - Information Sharing in government
  - Voluntary private-public partnerships related to cyber threats
  - Cross-border Data Flows
  - Encryption vs. law enforcement has been subject to debate in Committees
  - Enhanced FTC and FCC oversight
  - Likelihood that Congress gives the FTC the authority to issue civil penalties for Section 5 violations (for which the FTC has asked repeatedly)?
  - Likelihood of data breach notification legislation (preempting state laws)?
  - Likelihood of substantive data security requirements on the commercial sector (for which the FTC has asked repeatedly)?

Past Executive Branch Actions

- EO 13691: set up mechanisms to promote the widespread use of information sharing and analysis organizations
- Cybersecurity National Action Plan: proposed revolving fund for modernizing federal IT and the appointment of a federal chief information security officer
- Presidential Policy Directive 41: describes how the federal government will respond to cybersecurity incidents affecting government and private-sector entities (framework of roles, responsibilities, and coordination)
- U.S. Cyber Incident Response Plan: “to foster unity of effort for emergency operations planning” and to help those affected by cyber incidents understand what resources federal agencies can provide.

Cybersecurity and Privacy in the Trump Administration

- "Major review on hacking" within first 90 days
- Develop a comprehensive plan "to protect America's vital infrastructure from cyberattacks and all other form of attacks"
- Rudy Giuliani to advise on cybersecurity and help convene a rotating panel of private-sector leaders
- Top White House and DHS roles?
- Cabinet nominees pledged to make cybersecurity a priority
- Sanctions against Russia?
  - Congressional inquiries into Russian hacking (Sen. Graham to lead new Subcommittee)

Questions?

Reed Freeman, Partner
reed.freeman@wilmerhale.com

Jonathan Yarowsky, Partner
jonathan.yarowsky@wilmerhale.com

Kirsten Donaldson, Counsel
kirsten.donaldson@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 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 will 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.*