FTC Policy and Enforcement on Privacy and Data Security

What to Expect During the Trump Administration

WILMERHALE

WILMER CUTLER PICKERING HALE AND

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 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 thi practice. Nomi also allowed consumers to opt out online and erroneously represented th users could opt out in stores.
- The Republican Commissioners have dissented from some of these stance
  - Concrete vs. speculative harm.
    - *In re Nomi*: Commissioner Ohlhausen (likely to be interim Chairwoman) dissented because (1) Nomi did not collect PI and thus did not have to offer an opt-out, and (2) its erroneous representation did not benefit Nomi or harm anybody. 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 consider the costs to consumers and businesses.

Privacy: Going Forward

- Under the new administration, the FTC is likely to bring privacy enforcemen actions based on deception only where misrepresentations are intentional and material to consumers' behavior.
  - *See, e.g., In re Educational Research Center of America, Inc.* (2003): ERCA collected P from middle and high school students, ostensibly to help colleges improve recruitment. However, ERCA shared PI with commercial entities for marketing purposes.
- It is likely to bring enforcement actions rooted in unfairness 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 in this space.
- There is likely to be increased skepticism of the need for, and efficacy of, ne legislation.

Data Security: Past Administration

- Under President Obama, the FTC has pushed the boundaries of Section 5 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's failed to reasonably protect consumer data—even though no consumer suffered any har 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 Sect 5 may well be unreasonable. *LabMD v. FTC*, No. 16-16270 (11th Cir. 2016).
- The FTC has also pushed the concept of "security by design."
  - Commissioner Wright criticized the IoT Report's focus on security by design as lacking a "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 action only where consumers suffered actual, tangible harm, or faced a serious ris 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 like to focus more on weighing the costs and benefits, rather than assuming tha more security is always better.
  - This will purport to result in reduced costs to businesses and greater innovation.