FTC Hearings on Competition and Consumer Protection in the 21st Century

September 2018

Privacy in Focus®

The Federal Trade Commission (FTC or Commission) has begun a series of hearings on Competition and Consumer Protection in the 21st Century. As Wiley Rein noted previously, this is a major initiative that will help shape the agency’s – and the entire federal government’s – approach on issues critical to the digital economy. More specifically, the wide-ranging hearings will be of interest to a multitude of companies across industries – touching everything from global privacy and data security, to legal and regulatory frameworks, big data, and emerging technologies and their uses.

FTC Chairman Joe Simons described the hearings as intended to facilitate “serious reflection and evaluation” so that the Commission will be “better able to promote competition and innovation, protect consumers, and shape the law, so that free markets continue to thrive.”

Preliminary Comments & Stakeholder Feedback

In advance of the hearings, the Commission sought comments in order to “examine whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy.”

Hundreds of comments were filed across 11 topics selected by the Commission. Commenters included Fortune 100 companies, business associations, privacy advocates, academic institutions, state attorneys general, and members of Congress. Several of the Commission’s selected topics relate to privacy and data security issues, including but not limited to:

- **Topic 2**: Competition and consumer protection issues in communication, information, and media technology networks
- **Topic 4**: The intersection between privacy, big data, and competition
- **Topic 5**: The Commission’s remedial authority to deter unfair and deceptive conduct in privacy and data security matters
A variety of commenters called for tighter rules and regulations related to privacy and data security. Several consumer advocacy groups argued that the Commission should formally ask Congress for greater authority related to rulemaking and levying penalties for privacy and data security violations. Others argued that informational harm, on which the FTC has held workshops, should not need to be proven by showing “substantial injury.”

Members of Congress weighed in on the side of greater regulation of privacy and data security. Rep. James Langevin encouraged the Commission to pursue new tools to better deter negligent handling of personal or sensitive data. He proposed that the FTC’s current remedial authority, under Section 5 of the FTC Act, may not adequately deter unfair and deceptive conduct in privacy and data security matters. Sen. Richard Blumenthal argued that “[i]n light of recent technological advances, we need a stricter legal and regulatory framework to protect consumer privacy.”

A group of state Attorneys General[1] emphasized the need to continue enforcing consumer protection laws related to privacy and data security. They contend that “consumer privacy and data security is an afterthought in product and service development. Industry often does not adequately invest in privacy and security. Consumer data has inherent value and the free market alone does not adequately protect sensitive data.”

Industry feedback, however, pushed back on many of these notions. AT&T noted that “the Commission has properly relied on industry and multi-stakeholder processes rather than one-size-fits-all, top-down government regulation,” and the Commission has “long supported a measured approach that protects consumers from genuine privacy abuses[.]” Further, AT&T wrote, “self-regulatory mechanisms are often superior to governmental mandates because, unlike prescriptive rules, multistakeholder processes provide the flexibility and speed necessary to address rapid technology and market changes.” BSA – The Software Alliance, pointed to the benefits of emerging technologies, highlighting that artificial intelligence and machine learning are “revolutionizing how companies monitor network security,” improving fraud detection and data security overall.

Some commenters praised the current U.S. approach to privacy, arguing that it is effective and does not need an overhaul. The Association of National Advertisers (ANA), for example, argued that “[t]he well-functioning U.S. privacy framework is composed of: (1) a federal regulatory scheme that is primarily sectoral and targeted; and (2) self-regulatory codes of conduct that effectively promote the responsible online and offline collection and use of data.” ANA, in promoting the U.S. approach to privacy, argued that alternative approaches, like the California Consumer Privacy Act of 2018, will have adverse impacts on both competition and consumer protection. Similarly, the Consumer Technology Association (CTA) noted that, “the FTC should continue to promote a flexible and technology-neutral framework for privacy and security.” Underscoring that “emerging fragmentation and inconsistent domestic and international regulatory approaches to privacy and security pose new challenges for companies and threaten to confuse consumers,” CTA argued that the Commission “should continue to encourage industry to collaborate in global standardization efforts to develop technological best practices and standards, and also promote regulatory harmonization to increase economics of scales.”
Many commenters emphasized that the Commission should support the harmonization of fragmented state, federal, and global privacy and data security regimes. BSA noted that “alone or with other agencies, and, crucially, in partnership with the industry stakeholders who are on the front lines of our defense against sophisticated cyber threats,” the FTC should consider ways in which it can help simplify the patchwork of complex and sometimes conflicting data security laws, rules, and standards. ACT – The App Association argued that policymakers should pursue a single, national standard for data security and that such a standard should incentivize innovation and allow for broad flexibility.

Other commenters also stressed the need for a balanced approach, aligning with the stated intention of Chairman Simons. The Computer and Communications Industry Association pointed to studies based on investments made in the tech sector in the European Union, arguing that “[p]rivacy laws and regulations can have an unintentionally adverse impact if they do not strike the correct balance between privacy and furthering innovation. Restricting companies’ use and collection of data may unintentionally impair commerce in the digital economy, and by implication, reduce investment.”

Hearing Schedule

On August 24, 2018, the FTC announced its opening round of hearings. The current schedule is as follows:

- **Hearing #1** – September 13-14: Review of Competition and Consumer Protection Landscape; Concentration and Competitiveness in U.S. Economy; Privacy Regulation; Consumer Welfare Standard in Antitrust; Vertical Mergers.
- **Hearing #2** – September 21: State of U.S. Antitrust Law; Mergers and Monopsony or Buyer Power.
- **Hearing #3** – October 15-17: The Identification and Analysis of Collusive, Exclusionary, and Predatory Conduct by Digital and Technology-Based Platform Businesses; Antitrust Framework for Evaluating Acquisitions of Potential or Nascent Competitors in Digital Marketplaces; Antitrust Evaluation of Labor Markets.
- **Hearing #4** – October 23-24: Innovation and Intellectual Property Policy.
- **Hearing #5** – November 6-7: Privacy, Big Data, and Competition.
- **Hearing #6** – November 13-14: Algorithms, Artificial Intelligence, and Predictive Analytics.

Looking Ahead

Currently, the FTC is seeking further comments on Hearing #1; these comments are due October 14, 2018.

On September 17, Wiley Rein is hosting a roundtable discussion with FTC Commissioner Maureen Ohlhausen. And on September 27, as part of the Outlook on Cyber speaker series, Wiley Rein is hosting Bilal Sayyed, Director of the FTC’s Office of Policy Planning, and James Cooper, Deputy Director for Economic Analysis in the FTC’s Bureau of Consumer Protection, for a discussion on the Commission’s recent privacy and data security initiatives, including the ongoing hearings.
