WINSTON & STRAWN LLP

BLOG

Antitrust Enforcers Broaden Their Scrutiny of Aggregated Customer Data from the Technology Sector to Multiple Industries

DECEMBER 12, 2019

As federal and state antitrust enforcers ramp up their investigations into the technology sector and the legal implications of its use of aggregated customer data, recent developments suggest enforcers may be broadening their data-related scrutiny beyond top technology companies to other industries. In prepared remarks for an October 19, 2019 hearing before the House Subcommittee on Antitrust, Commercial, and Administrative Law, FTC Commissioner Rohit Chopra stated that firms "desperate for [consumers'] data" include "not just the Big Tech companies," but also "telecommunications companies," listing several firms, and "the automotive industry," which already is the subject of another DOJ antitrust probe. Chopra concluded that it would be desirable for the FTC to use its authority under Section 6 of the FTC Act to "conduct industrywide investigations and studies and mak[e] its findings available to the public," to ensure the FTC is operating on "deep knowledge and expertise of a particular market."[1]

Consistent with such a broadening of government antitrust scrutiny, the *New York Times* reported that the U.S. House of Representatives recently sent letters to "more than 80 companies . . . rang[ing] from smaller firms in retail and advertising to large corporations in entertainment, software and social media," seeking information "about their own businesses" as well as how top "tech companies may have engaged in anticompetitive behavior."

Chopra explained that one of the core concerns driving antitrust enforcers' scrutiny of aggregated user data was with "network effects"—simply put, the fact that "it is clunky for [app users] to check many different apps, [so] their best bet is to use the platform that everyone else is using." As users are "lured to the platform, this attract[s] more" users, which makes the platform's aggregated user data more valuable to advertisers and others. The D.C. Circuit explored the antitrust implications of network effects in its seminal opinion in *United States v. Microsoft*:

> In markets characterized by network effects, one product or standard tends towards dominance, because the utility that a user derives from consumption of the good increases with the number of other agents consuming the good. For example, an individual consumer's demand to use (and hence her benefit from) the telephone network increases with the number of other users on the network whom she can call or from whom she can receive calls. Once a product or standard achieves wide acceptance, it becomes more or less entrenched. Competition in such industries is "for the field" rather than "within the field." . . . [T]here is no consensus among commentators on the question of whether, and to what extent, current monopolization doctrine should be amended to account for competition in technologically dynamic markets characterized by network effects.

> Indeed, there is some suggestion that the economic consequences of network effects and technological dynamism act to offset one another, thereby making it difficult to formulate categorical antitrust rules absent a particularized analysis of a given market.[2]

With both federal and state antitrust enforcers investigating top U.S. technology companies, and scrutinizing other sectors where the major players have accumulated large and valuable datasets, courts soon may start deciding the antitrust ramifications of such "network effects" for companies in multiple industries—and, potentially, the types of remedies to deploy. Chopra suggested that appropriate federal and state remedies for anticompetitive misuse of data may include "opening up the intellectual property rights to underlying technologies that power a marketplace," as well as "voiding certain one-sided, take-it-or-leave it contract terms that are typically enforced by our courts," listing a number of historical examples of such antitrust remedies. Similar themes were echoed at the October 19th hearing discussed above in bipartisan commentary by House Subcommittee Members, as well as E.U. and other international enforcers.

This apparent broadening of government antitrust scrutiny of aggregated data and "network effects" to additional industries, coupled with the severity of potential remedies being contemplated by enforcers, raises significant risks and uncertainties for companies reliant upon valuable proprietary datasets. These risks and uncertainties are amplified by the fact that antitrust and competition law surrounding large aggregations of data is relatively undeveloped. The resolution of these disputed antitrust questions involving aggregated data will have major long-term implications for companies across industries. Such companies likely would be prudent to develop effective legal strategies for managing and minimizing this risk now at an early stage.

While the appropriate legal strategy for any given company will depend upon its individual circumstances, and it is impossible to say definitively what types of conduct federal and state enforcers will investigate and challenge in the future, reasonable predictions in that regard can be made based on the types of conduct that have been challenged by competition authorities in Europe, where enforcement in these areas ramped up several years earlier than in the United States. Several such practices involving aggregated data that potentially may be the subject of government scrutiny are set forth below:

- A firm produces both a market-dominant Product A and a Product B in a different product market, and uses data collected from Product A to support selling Product B, or vice versa.
- A firm's Product A enjoys a dominant market position due in part to its aggregated data, and the firm conditions use of Product A on using or otherwise favoring a Product B produced by the same company.
- A firm has a market-dominant platform on which there are sales or advertisements of both its own and other companies' products, and the firm favors its own products on its platform—particularly if there are barriers to challenging that platform's market dominance due to its aggregated data.

To assess whether specific conduct involving aggregated data might raise potential antitrust issues for a company, this typically would require a legal and factual analysis of the company's individual circumstances—for example, the market in which it competes, its competitors, the type of data it has, how that data was acquired, and the competitive justifications for its data-related practices. Government antitrust enforcers ask similar questions in conducting their own investigations, and in light of the apparent enforcement priorities today, it likely would be prudent for companies with important datasets to be prepared for that scenario.

---

[1] Specifically, FTC Act § 6 empowers the FTC to compel companies to provide information about their "organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals" and allows the FTC to make such information public. 15 U.S.C. § 46(b), (f).

[2] *United States v. Microsoft*, 253 F.3d 34, 49-50 (D.C. Cir. 2001), *cert. denied*, 534 U.S. 952 (citations and punctuation omitted).

5 Min Read

Authors

Susannah Torpey

Mark Rizik, Jr.

Related Locations

New York | San Francisco

Related Topics

Antitrust Intelligence | FTC | Government Enforcement | Disruptive Technology

Related Capabilities

Antitrust/Competition | Technology Antitrust | Technology, Media & Telecommunications

Related Regions

North America

Related Professionals

Susannah Torpey

Mark Rizik

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.