WINSTON & STRAWN LLP

BLOG

A New Antitrust Class Action Threat: Anticompetitive Invasion of Privacy

DECEMBER 22, 2020

Antitrust, data privacy, unfair competition, and class actions are among the pillars of consumer protection law. At the same time that federal government agencies and state attorneys general launch investigations and litigations targeting "Big Tech," the plaintiffs' class action bar is brainstorming and testing novel theories of competitive harm that unite antitrust and data privacy. In light of these recent activities, companies that use consumer data in their business operations must take heed of the uncertain legal landscape that is evolving to meet technological advances in data analytics.

In recent weeks, multiple class action lawsuits have been filed against Facebook for alleged antitrust violations for infringing upon user privacy. The complaints allege, among other things, that Facebook abuses its market dominance by violating user privacy and maintaining monopoly power by deceiving consumers and acquiring rivals, nascent rivals, or potential rivals. The class actions follow lawsuits brought by each of the Federal Trade Commission and 48 state attorneys general, both alleging that Facebook engages in anticompetitive tactics to either acquire or kill off its rivals.[1]

One of the recent lawsuits filed on December 9, 2020, by Facebook's users, marketers and direct buyers of advertisements exemplifies the legal claims against the social media company.[2] The private putative class action is especially notable because it puts forward a novel theory of antitrust harm—that Facebook (a service that is "free" from a monetary price perspective) has abused its market power by charging an increased quality-adjusted price for a product that is substantially degraded in quality due to privacy violations. The complaint alleges that Facebook's erosion of privacy protections is not just a consumer protection harm, but also an antitrust harm. According to the putative class members, they must adhere to Facebook's privacy policies if they want to participate in social media because of Facebook's market dominance achieved through ownership of various social media platforms. Moreover, plaintiffs allege that Facebook's privacy policies are difficult for consumers to understand, that Facebook deliberately obfuscates users' ability to know the nature and extent of the data it collects, and that it inhibits changes to privacy preferences by hiding them among dozens of other types of user preferences. All of this, plaintiffs allege, has resulted in the elimination or reduction of competition for users on the basis of privacy in the social network market and social media market. As a result, Facebook causes its users "to pay a higher data price than they would freely choose."[3]

The class actions are notable because they bridge a divide between regulation of privacy and competition. These areas of law have long been the source of debate among legal experts and policy-makers—with many remarking on a perceived tension between them.[4] For example, by overregulating privacy, incumbent firms such as Facebook or other "Big Tech" companies could hypothetically hamper market entry by withholding data that new entrants need to effectively compete.[5] On the other hand, allowing new entrants to access incumbent firms' data could compromise user privacy.[6] The putative class action against Facebook characterizes those tradeoffs as a false choice, claiming that antitrust and privacy issues must be considered together.

Although pursuing an antitrust cause of action for privacy violations may be a novel theory in the United States, German regulators previously challenged Facebook for essentially the same reasons. The German authority alleges in early 2019 that because of "Facebook's large market share, consumers have no choice but to relinquish their privacy to be part of the social network."[7] As a result, the German authority prohibited Facebook from associating data from applications like WhatsApp or Instagram with the main platform unless a person specifically agreed to the association.

Whether the plaintiffs' suits will be successful remains to be seen. Nonetheless, these actions could mark the beginning of a new frontier of class action lawsuits against large technology companies alleging privacy violations as an antitrust harm. For that reason, companies that utilize consumer data for their business should be aware of regulators' and civil litigants' increased focus on their conduct—especially if they could be alleged to have market power. Specifically, companies should be cognizant of five types of conduct in relation to data that could be construed as exclusionary: refusal to provide access to data; discriminatory access; exclusive contracts; tied sales and cross-usage; and discriminatory pricing. Other ways companies can protect themselves include: maintaining a record of the use and objectives of relevant databases that is updated as objectives change and evolve; assessing whether competitors have access to comparable data they need to offer comparable products or services; and considering expanding traditional antitrust compliance programs and training to address the relevant antitrust and privacy considerations raised by a company's use of data, such as reexamining privacy policies and providing training to employees beyond the salesforce to those working with gathering, collecting, contracting and using data or the algorithms that analyze the information.

---

[1] Complaint, *Federal Trade Commission v. Facebook, Inc.* (filed Dec. 9, 2020), *available at* https://www.ftc.gov/system/files/documents/cases/1910134fbcomplaint.pdf; Complaint, *State of New York, et al. v. Facebook, Inc.* (filed Dec. 9, 2020), *available at* https://ag.ny.gov/sites/default/files/facebook_complaint_12.9.2020.pdf.

[2] *Sherman, et al. v. Facebook, Inc.*, No. 5:20-cv-8721, Dkt. 1, ¶¶ 56-62 (N.D. Cal. Dec. 9, 2020).

[3] *Id.* ¶ 61.

[4] *The Tension Between Competition and Tech Are Gaining Global Attention*, EPIQ, July 15, 2020, *available at* https://www.epiqglobal.com/en-us/thinking/blog/tension-between-competition-and-tech (arguing "In the modern era, almost everyone needs access to data and the latest technology for both business and personal reasons. Because of this, individuals may continue to use certain services even if privacy is compromised. When a provider dominates the market, it has the ability to skimp on privacy protections and users will have no comparable competitors available. All of this makes policing big tech extremely difficult, as regulators have to balance privacy and competition issues. Deciding which issue should have more weight seems like an impossible task").

[5] Matthew Lane, *Recognizing and Dealing with the Tension between Competition and Privacy Policies*, Disruptive Competition Project, Oct. 22, 2019, *available at* https://www.project-disco.org/privacy/102219-recognizing-and-dealing-with-the-tension-between-competition-and-privacy-policies/ (noting that steps taken to prevent privacy breaches "can actually have an impact on competition goals.").

[6] *Id.* (stating that an argument exists that "new entrants need access to incumbents' data in order to compete, but the sharing of this data raises privacy concerns").

[7] Alex Matthews and Catherine Tucker, *Privacy Policy and Competition*, 4, The Brookings Institute, Dec. 2019, *available at* https://www.brookings.edu/wp-content/uploads/2019/12/ES-12.04.19-Marthews-Tucker.pdf.

5 Min Read

Author

Jeffrey J. Amato

Related Locations

New York

Related Topics

Antitrust Intelligence

Disruptive Technology

Private Civil Antitrust Litigation

Related Capabilities

Antitrust/Competition

Technology Antitrust

Technology, Media & Telecommunications

Related Regions

North America

Related Professionals

Jeffrey J. Amato

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.