

Consumer Data Monetization: The Antitrust Risks You Need to Know

APRIL 18, 2023

The collection, monetization, analysis, and use of consumer data have become ubiquitous aspects of modern business in the digital age. Companies, big and small, rely on consumer data to develop targeted advertising campaigns, enhance customer experiences, and create innovative products and services. However, the increasing reliance on consumer data also presents significant and growing antitrust risks for companies operating in the digital sphere.

The head of the U.S. Department of Justice (DOJ) Antitrust Division, Assistant Attorney General Jonathan Kanter, recently [revealed](#) that the DOJ would hire more data experts to help investigate antitrust violations related to consumer data. This development highlights the government's growing concern over antitrust violations in the tech industry, particularly those related to the aggregation of consumer data by businesses.

Consumer data is becoming increasingly relevant to competition assessments, primarily in two ways. First, privacy and data protection are emerging as important non-price components of competition. Consumers are becoming increasingly aware of the value of their personal information and are placing greater emphasis on privacy and data protection when making purchasing decisions. As a result, businesses that offer better privacy and data protection features may have a competitive advantage over those that do not.

Second, the collection, ownership, and access to consumer data can impact competition in the market. Companies that have access to more data may be able to offer better products and services and may also have an advantage in terms of marketing and advertising. This disparity can also create barriers to entry for smaller competitors who do not have access to the same amount of data.

As the DOJ expands its focus on data-related antitrust violations, companies that collect, monetize, and use consumer data will likely face heightened scrutiny and risks. Some of the antitrust risks that such companies may face include:

1. **Government investigations:** Companies that aggregate, monetize, and use consumer data could be subject to increased government investigations and scrutiny from regulators at the DOJ, Federal Trade Commission (FTC), state Attorneys General, or international foreign government enforcers such as the European Commission. The DOJ's move to hire more data experts indicates that it is preparing to take a closer look at companies that engage in anticompetitive behavior related to consumer data and competition over data privacy. Other enforcement

agencies around the globe are similarly showing interest in examining the competition issues at play in the data arena.

2. **Difficulty obtaining merger approval:** Mergers between businesses that use consumer data may face more difficulty obtaining approval from regulators. Data and privacy are now seen as nonprice components of competition that are evaluated by regulators scrutinizing transactions. Regulators may view companies that own vast amounts of consumer data as having an unfair advantage over competitors and may be hesitant to approve mergers that could further entrench a company's dominant position in the relevant markets. Data aggregation in markets could be viewed as potentially harmful to competition in at least two ways: 1) by reducing the quality of data protection and privacy in the relevant market; or 2) by raising barriers to entry or raising rivals' costs through the merging of consumer databases. Concerns about mergers reducing competition in respect of privacy might be especially relevant in zero-price markets where competition is largely on elements of quality rather than price.
3. **Monopolization:** Companies that aggregate and use consumer data to gain a dominant position in a market may face antitrust risks related to monopolization. The use of data to exclude competitors or limit consumer choice can be viewed as anticompetitive conduct that violates antitrust laws.
4. **Collusion:** Agreements between competitors are always suspect, and when it comes to consumer data there is no exception to that rule. Sharing sensitive consumer data with competitors can be subject to scrutiny by the DOJ and viewed as evidence of an agreement to restrain competition, which could be problematic under the antitrust laws. As we discussed in a [prior Competition Corner post](#), recent DOJ actions, including the withdrawal of longstanding policy statements, reflect a heightened interest in scrutinizing information exchanges among competitors.
5. **Price fixing:** It is per se illegal for competitors to coordinate prices. Using consumer data to set prices or coordinate pricing can be viewed as an agreement to fix prices, which violates antitrust laws. For example, coordinating or setting prices through a common data set or through agreed-upon algorithms or other artificial intelligence is akin to face-to-face meetings where competitors illegally fix prices. The DOJ has recently [expressed concern over the use of pricing algorithms by competitors](#), which can potentially lead to tacit or express collusion in the marketplace, resulting in higher prices or a weakening of competition. The agency cites studies showing the negative impact of such algorithms on competition and points to a criminal case involving the use of pricing algorithms in the online wall posters market as an example of how algorithms can facilitate collusion. These remarks highlight the need for companies to be cautious in their use of pricing algorithms and to ensure that their practices do not violate antitrust laws.
6. **Tying and bundling:** Companies that aggregate and use consumer data to tie or bundle products or services may face antitrust risks. Tying or bundling products or services with data can be viewed as an attempt to force customers to purchase unwanted products or services, which violates antitrust laws.
7. **Price discrimination:** When companies aggregate and use consumer data to set prices, they may be at risk of violating the Robinson-Patman Act—a law [the FTC has said](#) it would resume enforcement of after decades of inactivity—if they engage in price discrimination. For example, if a company uses consumer data to offer lower prices to certain customers or groups of customers while charging higher prices to others, it may be engaging in price discrimination that violates the Act. In addition, the use of consumer data to target specific customers or groups of customers with different pricing or promotional offers can also raise concerns under the Robinson-Patman Act. If the use of data results in price discrimination, it may be viewed as an unfair competitive practice that violates the Act.
8. **Private litigation risks:** Companies that engage in anticompetitive behavior related to consumer data may face civil litigation risks from competitors, consumers, and regulators concerning the points raised above. For example, a competitor may file a lawsuit alleging that the company engaged in anticompetitive behavior regarding the use of consumer data that harmed its business. Consumers may also file lawsuits alleging that the company violated the antitrust laws, entered agreements concerning data that unreasonably restrained commerce, violated their privacy rights, or engaged in other deceptive practices related to their data.

Risk Mitigation Practices

To mitigate the antitrust risks involved with aggregating, monetizing, and using consumer data, companies should ensure that their practices are transparent, ethical, and compliant with antitrust laws. This includes monitoring regulatory and legal developments related to consumer data and making necessary adjustments to their compliance policies and business practices. It is important for companies to be proactive in addressing these risks to avoid costly investigations, litigation, and reputational damage, while also promoting a more competitive and fairer marketplace for all. The recent move by the DOJ to hire more data experts highlights the growing concern over antitrust violations related to consumer data, making it essential for companies to be aware of these risks and take necessary steps to mitigate them.

5 Min Read

Author

[Jeffrey J. Amato](#)

Related Locations

New York

Related Topics

Antitrust Basics

Department of Justice (DOJ)

Compliance and Counseling

Technology Antitrust

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.