



# Compliance Guidance for Third-Party Data in the Wake of Antitrust Safe Harbor Repeals

Nearly a year after the U.S. Department of Justice revoked long-standing safe harbor policies<sup>1</sup> for information sharing relating to antitrust enforcement, many organizations remain uncertain about whether their data practices are compliant. While the loss of safe harbors doesn't automatically make data sharing unlawful, it signals a potential increase in scrutiny over the use of data collected and managed by a third-party.

The DOJ's decision to remove data sharing safe harbor policies<sup>2</sup> is one of many recent moves in the agency's ongoing campaign to strengthen antitrust enforcement and increase its sophistication in data use, analysis and regulation. The repeal follows guidance updates regarding corporate data<sup>3</sup> as a factor in maintaining, demonstrating and investigating compliance, and DOJ hiring of former compliance officials and experts in data and analytics.<sup>4</sup>

## A Look Back at Safe Harbors

Previously, several health care antitrust policy statements collectively established a safe harbor where the exchange of price and cost information would not be challenged "absent extraordinary circumstances," and provided that the data sharing activities stayed within the bounds of established approved parameters, including<sup>5</sup>:

- Sharing only information that was more than three months old;
- had been anonymized to obfuscate the identity of the sources;
- was combined from a minimum of five competitors to prevent linking particular data to an individual source.

Provided that companies and competitors followed these policies when exchanging information that would otherwise be considered competitively sensitive info (e.g., payment terms, pricing, etc.), they would not be viewed as engaging in anticompetitive or price fixing behaviors. Generally, these rules were applied by antitrust authorities to guide information sharing activities in other industries as well.<sup>6</sup>



## The New Take on Data and Pricing Algorithms

The agency's broad recognition of the changing role of data in corporate activities and compliance is a key underlying factor in the safe harbor repeal, with the authorities specifically acknowledging<sup>7</sup> that today's use of data makes it much easier for organizations to potentially manipulate or reverse engineer data more easily. Assistant Attorney General Doha Mekki of the Antitrust Division said in 2023, "The safety zones were written at a time when information was shared in manila envelopes and through fax machines. Today, data is shared, analyzed, and used in ways that would be unrecognizable decades ago. We must account for these changes as we consider how best to enforce the antitrust laws."<sup>8</sup>

Antitrust agencies are also increasingly focused on the use of pricing algorithms<sup>9</sup> and whether such use amounts to illegal, anticompetitive information sharing when the pricing software recommends prices based on competitor pricing data. During the most recent ABA Fall Forum, an antitrust official at the DOJ said, "The rise of algorithmic pricing is expanding the possibility of anticompetitive price coordination beyond concentrated markets to highly diverse sectors where collusion, tacit or otherwise, may have previously been impossible."<sup>10</sup>



Additionally, numerous lawsuits have been filed, alleging that the use of shared pricing data is a form of price-fixing and/or collusion. While at least one such case has been dismissed on procedural grounds, these trends suggest that potential plaintiffs and regulators will increase their focus on how organizations are using pricing algorithms.

While advancements in third-party data and information exchanges have created new concerns for regulators and in turn new antitrust risk for companies, they can also offer digital insights that support compliance efforts. For instance, the shift away from hard-copy records and reports to electronic data enables more advanced use of analytics and dashboards that make it easier for compliance teams to track what's happening across their organization and how sensitive information is being received, disseminated and utilized. For instance, by shifting hard copy reports to dashboards, companies can more easily restrict access to data such as by removing visibility of the most sensitive (*e.g.*, timeliest, most disaggregated) datapoints and limiting the number of users with access to competitive data to ensure using the new tools uphold antitrust compliance.

### Robust Data Compliance

With the DOJ's position that former safe harbor rules are no longer sufficient to protect competition and do not reflect the current business and data landscape, companies must reassess their compliance posture.

The repeal doesn't mean that all information sharing or pricing software is automatically illegal or anticompetitive, but it does mean that companies must take extra steps to scrutinize information sharing through the lens of the DOJ's most recent guidance and mitigate the related risks. The parameters outlined in the previous safe harbors — sharing only information that was more than three months old, had been anonymized to obfuscate the identity of the sources and was combined from a minimum of five competitors to prevent linking particular data to an individual source — can still serve as a benchmark against which to review data sharing practices. But they cannot be relied upon as a guarantee of compliance.

Further examination of how existing and future data sharing practices may impact antitrust compliance in an environment without safe harbors may involve one or more of the following steps:

- **Interview employees to capture how data is being used across functions.** Compliance teams need to fundamentally understand the internal data landscape within their organizations, including who is using what data, what sources are supplying it and how it influences go-to-market decisions. Before compliance can evaluate the potential antitrust risk of market data (including third-party software utilizing market data), it must understand the breadth of competitive data being employed by the organization. In interviews, employees should be asked about what data they're looking for, from whom they receive this data, how they view its value, what the output is after they review it, how current it is, how often they rely on the information and whether customers also have access to it. If there aren't clear answers to these questions, or there are significant gaps and inconsistencies in how employees are answering, that should be considered as a red flag for compliance to investigate further.



With the insights from interviews, compliance can take practical steps to reshape the use of data in a way that supports legitimate data analysis without risking potential antitrust violations or illegitimate uses. This may include improved controls, increased data aggregation and new policies.

- **Review current use of third-party data and implement safeguards to prevent data from being exported and shared outside of approved means.** While there is no longer a safe harbor for information sharing, the previous policies still serve as a guide for what type of data is most likely to raise antitrust concern. Organizations should continue to assess the currency and level of aggregation of competitor data and manage the type of data made available to employees. For example, compliance can leverage online reporting tools to digitize and manipulate the data to restrict the most sensitive information by further aggregating datapoints available, removing sensitive datapoints that are not relevant to business performance, and restricting from view the most disaggregated or current data. Restrictions can also be implemented to limit access only to certain business units or individuals within the organization. Ultimately, these controls will reduce the risk of violations, better secure sensitive information and strengthen the overall compliance program.
- **Evaluate the design and use of pricing algorithms.** The evaluation of third-party pricing algorithms, employed by two or more competing firms, is often discussed in terms of a hypothetical in which the tool was replaced with a person (Bob), and they were doing the same thing as the technology. The relevant questions then become: If every competitor gives their pricing information to Bob, they run the figures, and send a report back to everyone, are the companies then setting pricing based on Bob's recommendations, or are they using Bob's report only as one datapoint in a broader set of information and assessments that determine pricing? Moreover, how would the effectiveness of Bob's recommendations change if some competitors did not submit their information?



Thus, the concern with algorithms is the extent to which pricing is being determined in large part, if not solely, on the use of otherwise confidential and competitively sensitive information. Compliance teams should evaluate the use of pricing algorithms through this lens — whether it’s merely a single input in a decision-making process or if it’s representative of a tacit agreement among competitors to use the algorithm’s recommended pricing.

To reduce the risk of scrutiny, organizations should assess how the software’s recommendations factor into ultimate pricing decisions, including what other information influences pricing decisions, and how prices have changed since the software’s implementation. Compliance teams should also consider working with experts to have their algorithms tested for bias, potentially inappropriate use and other red flags.

The loss of data sharing safe harbors has created a new wave of uncertainty in an already challenging antitrust environment. Organizations are dealing with increased scrutiny in parallel with the requirement to respond to new complexities and digital risks. Reducing those risks will require a proactive and intelligent approach to data — understanding it, governing it and leveraging it. Although safe harbors are no longer a functional safety net, they still provide a sound benchmark or starting point of best practices for compliance teams that are getting started with examining their organization’s information sharing activities.



©2024. Published in *Antitrust Committee Articles*, April 11, 2024 by the American Bar Association. Reproduced with permission, all rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association or the copyright holder.

## Authors

### ADAM BERRY

Senior Managing Director

+1.212.651.7104

[adam.berry@fticonsulting.com](mailto:adam.berry@fticonsulting.com)

### ANDREA LEVINE

Managing Director

+1.212.499.3617

[andrea.levine@fticonsulting.com](mailto:andrea.levine@fticonsulting.com)

*The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.*

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. ©2024 FTI Consulting, Inc. All rights reserved. [fticonsulting.com](https://www.fticonsulting.com)



- 
- 1 U.S. Department of Justice, “Justice Department Withdraws Outdated Enforcement Policy Statements,” February 3, 2023, <https://www.justice.gov/opa/pr/justice-department-withdraws-outdated-enforcement-policy-statements>
  - 2 U.S. Department of Justice, “Statement of Antitrust Enforcement Policy Regarding Accountable Care Organizations Participating in the Medicare Shared Savings Program,” October 20, 2011, <https://www.justice.gov/sites/default/files/atr/legacy/2011/10/20/276458.pdf>
  - 3 U.S. Department of Justice, “Evaluation of Corporate Compliance Programs,” March 2023, <https://www.justice.gov/criminal-fraud/page/file/937501/download>
  - 4 *Corporate Compliance Insights*, “The DOJ Doubles Down on Data, Raising the Stakes for Proactive Information Governance,” October 19, 2022, <https://www.corporatecomplianceinsights.com/doj-data-governance/>
  - 5 The Federal Trade Commission/U.S. Department of Justice, Statement of Antitrust Enforcement Policy Regarding Accountable Care Organizations Participating in the Medicare Shared Savings Program, October 20, 2011, <https://www.justice.gov/sites/default/files/atr/legacy/2011/10/20/276458.pdf>
  - 6 Arnold & Porter, “No Safe Harbors: DOJ Signals Increased Scrutiny of Information Exchanges,” February 14, 2023, <https://www.arnoldporter.com/en/perspectives/advisories/2023/02/no-safe-harbors-doj-signals-increased-scrutiny>
  - 7 U.S. Department of Justice, “Principal Deputy Assistant Attorney General Doha Mekki of the Antitrust Division Delivers Remarks at GCR Live: Law Leaders Global 2023,” February 2, 2023, <https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-doha-mekki-antitrust-division-delivers-0>
  - 8 U.S. Department of Justice, “Principal Deputy Assistant Attorney General Doha Mekki of the Antitrust Division Delivers Remarks at GCR Live: Law Leaders Global 2023,” February 2, 2023, <https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-doha-mekki-antitrust-division-delivers-0>
  - 9 American Bar Association, “The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Antitrust Enforcement,” 2017, [https://www.ftc.gov/system/files/documents/public\\_statements/1286183/mcsweeny\\_and\\_odea\\_-\\_implications\\_of\\_algorithmic\\_pricing\\_antitrust\\_fall\\_2017\\_0.pdf](https://www.ftc.gov/system/files/documents/public_statements/1286183/mcsweeny_and_odea_-_implications_of_algorithmic_pricing_antitrust_fall_2017_0.pdf)
  - 10 *Law360*, “AI Could Expand Price-Fixing To Less Concentrated Markets,” November 9, 2023, <https://www.law360.com/articles/1765541/ai-could-expand-price-fixing-to-less-concentrated-markets>