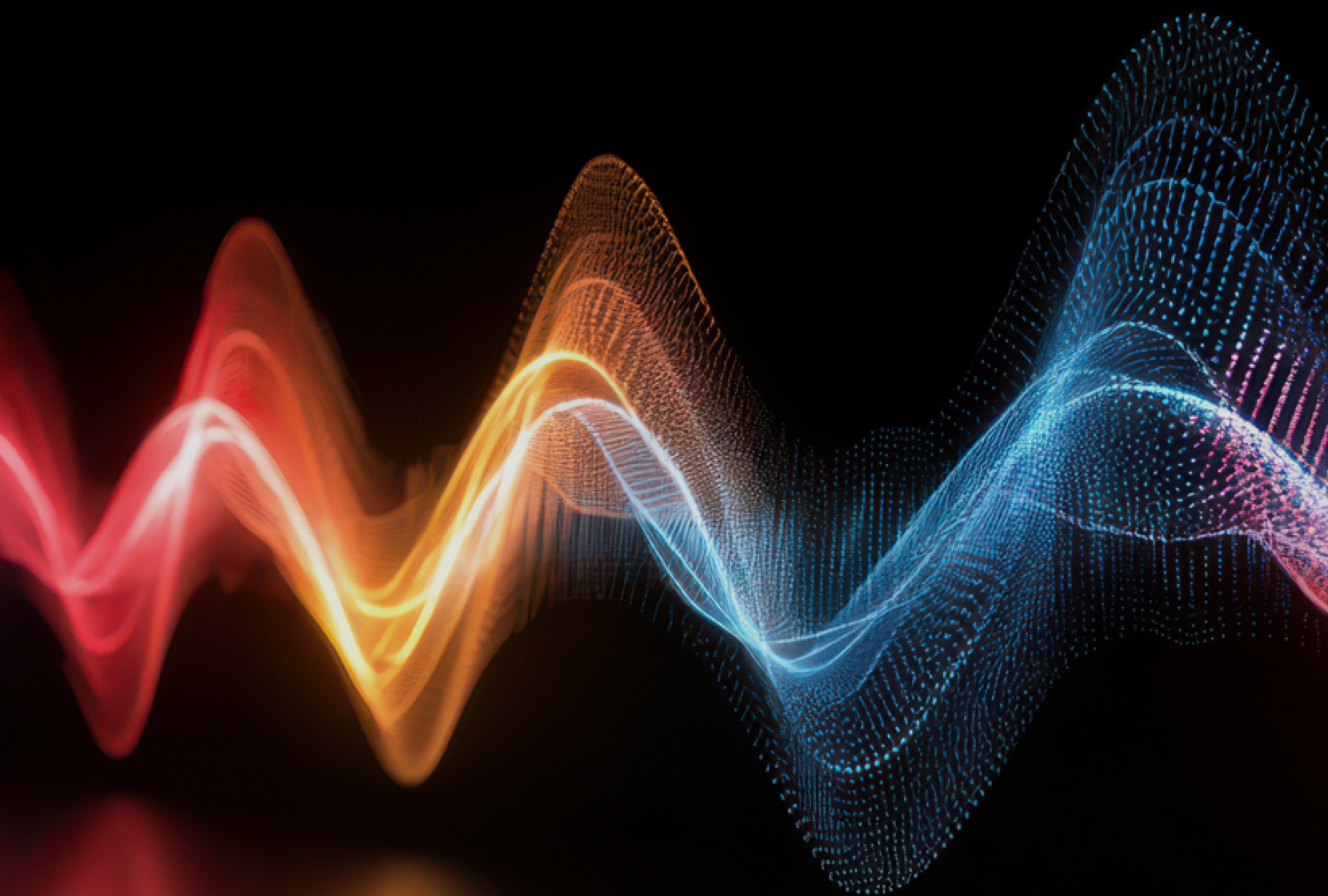
ANTITRUST COMPLIANCE FOR THE AI PRICING ERA



BY ALEJANDRA URIA & ANDRE GEVEROLA[1]

1 Arnold & Porter.

CPI ANTITRUST CHRONICLE July 2026

ANTITRUST COMPLIANCE FOR THE AI PRICING ERA

By Alejandra Uria & Andre Geverola

The use of algorithmic and artificial intelligence tools to assist businesses with pricing decisions has generated unprecedented antitrust scrutiny across federal agencies, federal courts, and state and local legislatures. This article surveys the major legal developments shaping the algorithmic pricing landscape—from the first federal appellate opinion on the issue in *Gibson v. Cendyn Group, LLC*, to DOJ consent decrees, to landmark state statutes in California and New York—and translates those developments into a practical compliance framework. The article explains that, despite doctrinal uncertainty, a coherent set of compliance principles has emerged: companies must preserve independent pricing judgment, scrutinize the data inputs of third-party software, avoid communications with competitors about the use of pricing software, and implement the governance structures necessary to monitor algorithmic decision-making on an ongoing basis. Companies that take these steps will be better positioned to demonstrate the hallmarks of an effective antitrust compliance program as articulated by the DOJ's November 2024 Guidance on the Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations ("DOJ Guidance").

I. INTRODUCTION

The adoption of algorithmic and artificial intelligence tools to assist with pricing decisions has transformed how companies compete across multiple sectors of the economy. Revenue management software that dynamically sets hotel room rates, platforms that recommend rents for residential apartment buildings, and healthcare data analytics services that benchmark physician reimbursement rates have become commonplace. Yet the more pervasive these tools have become, the more intensely they have attracted antitrust scrutiny from federal enforcers, state attorneys general, and private plaintiffs.

The antitrust landscape governing algorithmic pricing traces its origins to a 2015 Department of Justice criminal prosecution of a UK online retailer for conspiring to fix prices through a common algorithm.[2] The risks resulting from algorithmic pricing have evolved rapidly and unevenly since then, accelerating dramatically after private plaintiffs filed the first civil algorithmic price fixing cases against software company RealPage, Inc. in 2022.[3] Courts have dismissed complaints, denied motions to dismiss, and applied competing liability standards to the same basic fact pattern. The U.S. Department of Justice, Antitrust Division ("DOJ") has filed Statements of Interest advancing aggressive theories of liability while simultaneously resolving its own civil suit through consent decrees that drew lines between permissible and impermissible uses of algorithmic pricing data. And California and New York recently became the first states to legislate directly in this space, enacting laws that restrict the use of competitor data in pricing algorithms. Municipalities from San Francisco to Hoboken have followed.

For companies that use — or are considering using — algorithmic pricing tools, the practical challenge is not merely to track these disparate developments, but to translate them into a workable compliance program for the business. This article attempts to do that. Part II surveys the key judicial decisions and enforcement actions that define the current legal landscape. Part III examines the DOJ's updated compliance guidance as it applies to algorithmic pricing. Part IV synthesizes these sources into a practical compliance framework. Part V concludes with observations about where the law may be headed.

II. THE LEGAL LANDSCAPE: COURTS, ENFORCERS, AND LEGISLATURES

A. The Judicial Framework: From RealPage to Segal

The fundamental question courts have grappled with is whether competing companies' shared use of an algorithmic pricing tool constitutes "concerted action" under Section 1 of the Sherman Act and, if so, whether such conduct is per se unlawful or instead subject to the rule of reason. Four cases have been most instructive, and they have reached different answers.

In *In re RealPage, Inc., Rental Software Antitrust Litigation,* the U.S. District Court for the Middle District of Tennessee denied a motion to dismiss a complaint alleging that apartment building owners and managers had conspired to inflate rental prices through algorithmic pricing software that employed aggregated competitor data to recommend prices.[4] The court found that because the software was alleged to be a "melting pot of confidential competitor information," the complaint plausibly alleged anticompetitive conduct.[5] The court declined, however, to apply per se liability — concluding instead that the rule of reason should govern, because the allegations were sufficiently novel to warrant balancing anticompetitive effects against potential procompetitive justifications.[6]

The U.S. District Court for the Western District of Washington in *Duffy v. Yardi Systems, Inc.* reached a more plaintiff-friendly result.[7] There, the court found that the complaint adequately alleged a per se unlawful horizontal price-fixing agreement because the competing apartment owners had allegedly accepted an invitation from the software provider to trade commercially sensitive pricing information in exchange

2 *United States v. Topkins,* No. 15-cr-00201 (N.D. Cal. Apr. 6, 2015).

3 Complaint, *Bason et al. v. RealPage, Inc. et al.*, No. 3:22-cv-01611-WQH-MDD (S.D. Cal. Oct. 18, 2022).

4 *In re: RealPage, Inc., Rental Software Antitrust Litig.*, 709 F. Supp. 3d 478 (M.D. Tenn. 2023).

5 *Ibid.* at 512.

6 *Ibid.* at 520 ("Moreover, courts are hesitant to apply the per se standard to new or 'novel way[s] of doing business' that have not yet been tested or studied by economists to conclusively determine that these types of conspiracies are per se anticompetitive.") (citing *In re Sulfuric Acid Antitrust Litig.*, 703 F.3d 1004, 1011 (7th Cir. 2012)).

7 *Duffy v. Yardi Sys. Inc.*, 758 F. Supp. 3d 1283 (W.D. Wash. Dec. 4, 2024).

for the ability to charge elevated rents without fear of undercutting by rivals.[8] The court reasoned that this conduct was sufficiently analogous to traditional price-fixing to warrant the per se rule, rather than a more forgiving rule-of-reason analysis.[9]

The Ninth Circuit's August 2025 opinion in *Gibson v. Cendyn Group, LLC,* marked the first federal appellate decision to address the antitrust implications of algorithmic pricing tools – and came to a different result.[10] The court affirmed dismissal of a complaint alleging that Las Vegas Strip hotels had engaged in a hub-and-spoke antitrust conspiracy by independently choosing to license the same pricing software from a common vendor.[11] The Ninth Circuit emphasized that Section 1 requires a causal link between the challenged agreement and an anticompetitive restraint of trade.[12] However, because the plaintiffs had abandoned their hub-and-spoke theory on appeal, the only agreements at issue were separate bilateral license agreements between each hotel and the software provider — agreements the court characterized as ordinary sales contracts that did not implicate antitrust liability.[13]

Critically, the *Gibson* court identified two circumstances in which algorithmic pricing might support a Section 1 claim. First, if competitors agreed among themselves to use the same software and follow its pricing recommendations, such a horizontal agreement would "undoubtedly" harm competition by eliminating each competitor's independent pricing incentives.[14] Second, the antitrust analysis might differ if the software allowed competitors to share confidential pricing information with each other.[15] Unlike the allegations in *RealPage*, the software in *Gibson* was not alleged to pool or share any hotel's confidential data to recommend pricing for other competitors.

Most recently, the Northern District of Illinois added another dimension to the legal landscape in *Segal v. Amadeus IT Group*, dismissing a Sherman Act § 1 claim against luxury hotel brands that used a software platform to share forward-looking, non-public occupancy, average daily rate, and revenue-per-available-room data with competitors in a "give to get" exchange.[16] The court held that information-sharing, even of sensitive non-public data, does not by itself satisfy the agreement element of a § 1 claim — rejecting the plaintiff's argument that the exchange of information alone establishes an antitrust conspiracy. Because Demand360's aggregated competitive sets gave subscribers no way to identify which hotels their competitors were observing, and because the alleged price-stabilization scheme lacked any enforcement mechanism, the court found that the third amended complaint alleged nothing beyond parallel conduct. The court drew an explicit contrast with *In re MultiPlan* where similar data-sharing allegations survived dismissal because the third-party provider was alleged to have acted as a "go between" facilitating collusion, underscoring that the hub-and-spoke structure, not the data exchange itself, is what transforms an information-sharing arrangement with a vendor into concerted action under § 1.[17]

Taken together, these four decisions reveal a judicial framework still very much in development. While courts agree that algorithmic pricing can, under the right circumstances, constitute unlawful concerted action, they have yet to coalesce around a consistent standard for when that threshold is crossed.

B. DOJ Enforcement: Statements of Interest and Consent Decrees

Against this shifting judicial backdrop, the Department of Justice has not waited for the courts to settle the law. Throughout these litigations, DOJ has played an active role, filing Statements of Interest in multiple cases to advance its views on the antitrust implications of algorithmic pricing.

---

8 *Ibid.* at 1292.

9 *Ibid.* at 1296-1297.

10 *Gibson v. Cendyn Grp.*, LLC, No. 24-3576, 2025 WL 2371948 (9th Cir. Aug. 15, 2025).

11 *Ibid* at 1076-1077.

12 *Ibid.* at 1077.

13 *Ibid.* at 1081-1082.

14 *Ibid.* at 1076.

15 *Ibid.* at 1083, n.8.

16 *Segal v. Amadeus IT Grp., S.A.*, No. 24-CV-1783, 2026 WL 879583, ECF No. 178 (N.D. Ill. Mar. 31, 2026).

17 *Ibid.* at 5 (citing *In re MultiPlan Health Ins. Provider Litig.*, 789 F. Supp. 3d 614, 641 (N.D. Ill. 2025) (involving allegations that healthcare providers' shared use of MultiPlan's algorithm to calculate out-of-network reimbursement rates constituted a hub-and-spoke price-fixing conspiracy that suppressed payments to providers below competitive levels; complaint survived dismissal because the third-party provider was alleged to have acted as a "go between" among the defendants, plausibly establishing concerted action under § 1)).

Under both the Biden and Trump administrations, DOJ has maintained that competitors' use of a common algorithm that sets recommended or starting-point prices can violate Section 1 of the Sherman Act even where competitors vary on their final pricing — and that an invitation proposing collective action, followed by conduct demonstrating acceptance, can establish an antitrust violation without a direct agreement among competitors.[18]

Most recently, DOJ filed a Statement of Interest in *In re Frozen Potato Products Antitrust Litigation,* a consolidated class action involving alleged information exchanges through a third-party data analytics platform.[19] There, DOJ pressed an expansive view, arguing that information exchanges can constitute "concerted action" under Section 1 where users of a third-party platform mutually expect to receive reciprocal information — and expressly resisted the suggestion that aggregated, anonymized, or backward-looking data is categorically less likely to produce anticompetitive effects.[20]

In addition to filing statements of interest in private plaintiff actions, DOJ has also filed civil suits alleging algorithmic price fixing. In August 2024, DOJ filed a civil lawsuit against rental revenue management software company RealPage and subsequently entered into proposed consent decrees with RealPage and several co-defendant property managers.[21] Those decrees are particularly instructive because they translate DOJ's enforcement priorities into specific operational requirements: RealPage was required to stop using non-public competitively sensitive information ("CSI") from unaffiliated properties in the runtime operation of its pricing software, subject to limited exceptions; prohibited from using non-public CSI to train future models, except for backward-looking unaffiliated property data that is at least 12 months old and not derived from active leases; and required to modify its software to eliminate asymmetric price floors, remove features that suppress price reductions, and ensure that all pricing recommendations are non-binding and can be overridden by users.[22] Property manager defendants were prohibited from using or sharing competitors' nonpublic CSI in rental pricing and from using any Revenue Management Product that relies on such CSI in its operation or model training.[23] One property manager was separately required to cease participation in RealPage user groups and committees, while another — which operated its own proprietary Revenue Management Product — was required to cease using all third-party Revenue Management Products by February 28, 2026, and prohibited from coordinating with other property managers or owners on the adoption of particular revenue management products.[24]

C. State and Local Legislation

Beyond the federal enforcement and litigation landscape, companies must now also navigate a rapidly expanding patchwork of state and local algorithmic pricing laws.[25] On October 6, 2025, California became the first state to amend its principal antitrust statute, the Cartwright Act, to address algorithmic pricing directly.[26] California Assembly Bill 325 makes it unlawful to use or distribute a common pricing algorithm as part of a contract, combination, or conspiracy to restrain trade, or to coerce another person to set prices based on a common pricing algorithm's recommendations.[27] The statute defines "common pricing algorithm" broadly to encompass any methodology used by two or more persons that uses competitor data — without distinguishing between publicly available and non-public data — to recommend, align, stabilize, set, or otherwise

18 Statement of Interest, *In re Multiplan Health Insurance Provider Litigation*, 24-cv-06795, ECF No. 382 (N.D. Ill. Mar. 27, 2025); *see also* Statement of Interest, *Duffy v. Yardi Sys., Inc.*, No. 2:23-cv-1391, ECF No. 149 (W.D. Wash. Mar. 1, 2024).

19 Statement of Interest of the United States, *In re Frozen Potato Products Antitrust Litig.*, 1:24-cv-11801, ECF No. 266 (N.D. Ill. Feb. 27, 2026).

20 *Ibid.* at 7-8, 12-13.

21 Complaint, *United States v. RealPage, Inc.*, 1:24-cv-00710, ECF No. 1 (M.D.N.C. Aug. 23, 2024); Press Release, DOJ, Justice Department Requires RealPage to End Sharing Competitively Sensitive Information (2025); Press Release, DOJ, Justice Department Reaches Proposed Settlement with Greystar, Largest U.S. Landlord (2025).

22 Proposed Final Judgment, *United States v. RealPage, Inc.*, 1:24-cv-00710, ECF No. 159-1 (M.D.N.C. Nov. 24, 2025).

23 Proposed Final Judgment, *United States v. Greystar Management Services LLC*, 1:24-cv-00710, ECF No. 152-1 (M.D.N.C. Aug. 8, 2025); Proposed Final Judgment, *United States v. LivCor LLC*, 1:24-cv-00710, ECF No. 164-1 (M.D.N.C. Dec. 23, 2025).

24 *Ibid.*

25 Cal. Assembly Bill 325, 2025–2026 Leg. (Cal.) (signed Oct. 6, 2025); Cal. Senate Bill 763, 2025-2026 Leg. (Cal.) (signed Oct. 6, 2025); N.Y. Gen. Bus. Law § 340-B (effective Dec. 15, 2025); N.Y. Gen. Bus. Law § 349-A (Algorithmic Pricing Disclosure Act); San Francisco Ordinance No. 224-24 (Oct. 2024); Philadelphia Bill No. 240823 (Oct. 2024); City of Minneapolis Ordinance No. 2025-010 (Apr. 2025); New Jersey City Ordinance 25-057 (May 2025); City of Providence Ordinance 48895 (May 2025); San Diego O-21955 (May 2025); Hoboken CC Ordinance Chapter 158-2 (July 2025); Seattle Council Bill No. 121000 (July 2025).

26 Cal. Assembly Bill 325, 2025–2026 Leg. (Cal.) (signed Oct. 6, 2025).

27 *Ibid.*

influence a price or commercial term.[28] California simultaneously increased Cartwright Act fines for corporate violators to the greater of six million dollars or twice the pecuniary gain to the violator.[29]

New York acted shortly thereafter, amending the Donnelly Act effective December 15, 2025 to prohibit residential rental property owners from using algorithms that perform a "coordinating function" — defined to include collecting competitor pricing data, processing that data (including by using it to train an algorithm), and recommending rental prices or lease terms.[30] At the municipal level, at least ten jurisdictions across the country — including San Francisco, Philadelphia, Minneapolis, Jersey City, Providence, San Diego, Hoboken, Seattle, Berkeley, and Portland — enacted ordinances restricting or prohibiting the use of algorithmic tools in setting residential rents, joining a wave of local regulatory action that began in late 2024.[31]

Against this backdrop of judicial decisions, enforcement actions, and expanding legislation, companies face growing pressure to demonstrate that their use of algorithmic pricing tools is both lawful in design and defensible in practice. Understanding how DOJ evaluates compliance programs — and what it now expects given the rise of AI-driven pricing technology — is therefore critical to navigating the legal landscape.

III. DOJ COMPLIANCE GUIDANCE AND ALGORITHMIC PRICING

In November 2024, DOJ published its updated Guidance on the Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations ("DOJ Guidance"), the first revision since 2019.[32] Although the DOJ Guidance is primarily addressed to criminal enforcement, DOJ has stated that it will apply the same principles in civil antitrust resolutions.[33] The DOJ Guidance addresses five dimensions of compliance program effectiveness: leadership, resourcing, reporting culture, technology, and civil application.

Most notable for companies using algorithmic pricing tools is the DOJ Guidance's treatment of new technologies. DOJ now expressly expects compliance functions to be involved in the deployment of AI and other algorithmic tools — not merely as a post-hoc check, but as part of the evaluation process before the technology is adopted.[34] The DOJ Guidance asks whether compliance personnel understand the AI and technology tools a company uses, and whether the compliance program monitors and detects decision-making by AI or other technology tools to ensure they are not violating antitrust laws.[35]

The DOJ Guidance also emphasizes continuous improvement: compliance programs should not be static but should be updated as risks evolve.[36] In the context of algorithmic pricing, this means that a company cannot treat its initial vetting of a software tool as a one-time exercise. As the legal landscape changes — as new cases are decided, new laws are enacted, and new features are added to existing software — companies must revisit and update their assessments.

28 *Ibid.* at Section 16729 (d)(3).

29 Cal. Senate Bill 763, 2025-2026 Leg. (Cal.) (signed Oct. 6, 2025).

30 N.Y. Gen. Bus. Law § 340-B (effective Dec. 15, 2025).

31 San Francisco Ordinance No. 224-24 (Oct. 2024); Philadelphia Bill No. 240823 (Oct. 2024); City of Minneapolis Ordinance No. 2025-010 (Apr. 2025); New Jersey City Ordinance 25-057 (May 2025); City of Providence Ordinance 48895 (May 2025); San Diego O-21955 (May 2025); Hoboken CC Ordinance Chapter 158-2 (July 2025); Seattle Council Bill No. 121000 (July 2025); Berkeley Ordinance No. 7956-N.S (March 2025); Portland Ordinance No. 192122 (Feb. 2026); RealPage has filed suits challenging these state and local restrictions on First Amendment and preemption grounds. *See, e.g.*, Complaint, *RealPage, Inc. v. City of Berkeley*, No. 3:25-cv-03004 (N.D. Cal. filed Apr. 2, 2025); Complaint, *RealPage, Inc. v. James*, No. 25-cv-9847 (S.D.N.Y. filed Nov. 25, 2025).

32 Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, U.S. Dep't of Justice, Antitrust Division (Nov. 2024), available at https://www.justice.gov/atr/media/1376686/dl [hereinafter DOJ Guidance].

33 *Ibid.* at 3 ("In seeking to resolve investigations into civil antitrust violations, companies . . . should expect the civil team to consider many of the same factors when assessing the effectiveness of their compliance program as criminal prosecutors do.").

34 *Ibid.* at 9-10 ("How does the company's risk assessment address its use of technology, particularly new technologies such as artificial intelligence (AI) and algorithmic revenue management software, that are used to conduct company business? As new technology tools are deployed by the company, does the company assess the antitrust risk the tools pose? What steps is the company taking to mitigate risk associated with its use of technology? Are compliance personnel involved in the deployment of AI and other technologies to assess the risks they may pose? Does the compliance organization have an understanding of the AI and other technology tools used by the company? How quickly can the company detect and correct decisions made by AI or other new technologies that are not consistent with the company's values?").

35 *Ibid.* at 9-10, 13 ("… Does the compliance program monitor and detect decision-making by AI or other technology tools to ensure they are not violating antitrust laws?").

36 *Ibid.* at 5, 9, 12, 13 (see, e.g. "Are compliance materials updated with recent developments and periodically refreshed so they do not become stale? Are the compliance program and compliance materials updated to account for newly developed technology and emerging risks?").

The DOJ Guidance's attention to ephemeral messaging and electronic communications is also relevant in this context.[37] DOJ is concerned with preserving evidence of potentially anticompetitive conduct, and companies that use algorithmic pricing tools in industries under scrutiny should ensure that communications about software adoption, data input decisions, and pricing strategy are conducted and preserved in accordance with clear document retention policies.

Warnings from DOJ enforcement leadership give teeth to the DOJ Guidance's requirements. In May 2026 remarks, Acting DAAG Daniel Glad cautioned that companies with AI governance processes focused solely on privacy, cybersecurity, and operational risk, without asking whether a pricing tool facilitates coordination with competitors, do not have a mature compliance program. "The model did it," he warned, "is not compliance. It is the beginning of the next question."[38] Glad further noted that advice of counsel is not a cognizable defense to a criminal Sherman Act violation, which does not require specific intent — meaning that legal sign-off on an algorithmic pricing tool does not insulate a company or its employees from criminal exposure. Finally, Glad underscored that the DOJ Guidance should be read alongside the Antitrust Division's Whistleblower Rewards Program, which creates a second race running parallel to the Antitrust Division's Leniency Program: engineers, data scientists, product managers, and compliance personnel who built or reviewed a pricing tool may have both the knowledge and the financial incentive to report to DOJ before the company does.[39] These developments signal DOJ's openness to criminal enforcement against algorithmic pricing software and the urgency with which companies must proactively address antitrust risks, both by building effective compliance programs and by moving quickly when self-reporting is warranted.

Taken together, the DOJ Guidance and DAAG Glad's remarks clarify the standard against which algorithmic pricing compliance programs will be measured. The following translates these expectations, together with the lessons of the judicial decisions and consent decrees discussed in Part II, into a concrete compliance framework that companies can implement today.

IV. A PRACTICAL COMPLIANCE FRAMEWORK

A. Preserve the Independence of Pricing Decisions

The central lesson of *Gibson,* the DOJ consent decrees, and the DOJ Guidance is that the antitrust analysis turns primarily on whether a company's pricing decisions are genuinely independent. A company may use algorithmic pricing software — even software used by competitors — provided that it makes an independent choice to do so; retains the ability to override, modify, or reject the software's recommendations; and does not use non-public competitor data in making pricing decisions. Compliance programs should therefore ensure, as an operational matter, that authorized users can manually set pricing parameters and override algorithmic recommendations without facing software-generated economic disincentives or penalties. Practically, this means that software functionality should be reviewed to confirm that the program does not impose pricing floors, does not suppress price reductions, and does not require users to accept recommended prices or price ranges.

B. Scrutinize Data Inputs

The distinction between publicly available data and non-public competitively sensitive information is another key issue in evaluating whether algorithmic pricing software poses antitrust risk. Both *Gibson* and the DOJ consent decrees converge on this point: the use of a common pricing algorithm is most legally defensible when the algorithm relies on publicly available pricing data — prices posted on websites, published by third-party aggregators, or otherwise available to any market participant — rather than on non-public information contributed by competitors.[40]

Companies should therefore conduct thorough due diligence on the data used by the algorithmic pricing tool before adoption, with particular focus on three questions: (i) What data inputs does the software use to generate recommendations? (ii) Does the software pool or aggregate non-public data contributed by multiple users, and if so, what is done with a particular company's data? (iii) Who else uses the software, and is there any mechanism by which one user's confidential pricing data could influence recommendations made to a competing user? The answers to these questions should be memorialized in writing and revisited whenever the software or its underlying data model is updated.

---

37 *Ibid.* at 5-6 ("What electronic communication channels do the company and its employees use, or allow to be used, to conduct business? How does the process vary by jurisdiction and business function, and why? What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels? Does the company have clear guidelines regarding the use of ephemeral messaging or non-company methods of communication including the extent to which those communications are permitted and when employees must preserve those communications? What preservation or deletion settings are available, and what is the rationale for the company's approach to what settings are permitted?").

38 Speech, DOJ, Acting Deputy Assistant Attorney General for Criminal Enforcement Daniel Glad Delivers Remarks at the Antitrust West Coast Conference (May 14, 2026).

39 *Ibid.*

40 *Gibson*, 2025 WL 2371948, at 1083, n.8.

Vendor agreements are an important lever here. Companies should insist on contractual provisions that describe, with specificity, what data inputs are used by the software, how the company's own non-public data will be used (and, critically, how it will not be used), and what restrictions apply to the vendor's use of company data for purposes of model training or providing recommendations to other customers. Robust antitrust compliance language should be included in all pricing vendor agreements.

C. Avoid Competitor Communications About Software Adoption and Use

Even where the underlying software is antitrust-compliant in its design, the *Gibson* court identified horizontal agreements among competitors about whether to use the software and how to use information from it as independently problematic.[41] Companies should therefore train their employees to avoid discussions with competitors — whether at industry conferences, through trade association activities, or in any other forum — about which algorithmic pricing tool to adopt, how to configure it, or how to respond to its recommendations.

This concern is not hypothetical. DOJ's consent decrees explicitly prohibited defendant property managers from agreeing with other owners or managers to adopt a pricing algorithm and from disclosing or obtaining non-public CSI through industry meetings or competitor communications. Companies that operate in industries where algorithmic pricing software is widely used should be especially alert to the risk that trade association activities could be construed as facilitating coordination about software adoption or use.

D. Integrate Compliance into the Technology Adoption Process

The DOJ Guidance's most significant contribution to algorithmic pricing compliance is its expectation that compliance personnel should be involved in the deployment of AI and algorithmic tools before the technology is adopted — not merely consulted after problems arise.[42] This represents a meaningful shift from a model in which legal review of pricing practices is episodic and reactive to one in which antitrust compliance is embedded in the product evaluation and vendor selection process.

Concretely, this means that when a business unit identifies a candidate algorithmic pricing tool, the compliance or legal function should be included in the evaluation team. That team should assess the tool against the criteria identified above (data inputs, override capability, software design), document its analysis, and obtain appropriate sign-off before the tool is deployed. Any material changes to the software — new features, changes to the underlying data model, expansion to new markets — should trigger a fresh compliance review.

Companies should also consider implementing ongoing monitoring of algorithmic decision-making. The DOJ Guidance specifically asks whether compliance programs monitor and detect decision-making by AI tools to ensure that those tools are not violating antitrust laws.[43] In practice, this might mean periodic compliance audits of the data inputs and outputs of pricing software, review of pricing recommendations against market benchmarks, and escalation protocols when the software generates recommendations that appear inconsistent with competitive market conditions.

While the federal compliance framework described above provides a strong foundation, the obligations companies face are no longer exclusively federal. As the state legislative developments described in Part II.C make clear, companies must include jurisdiction-specific compliance obligations in their antitrust compliance programs — and must do so across a rapidly expanding and non-uniform set of state and local requirements.

E. Monitor State and Local Regulatory Developments

The California and New York statutes, and the wave of municipal ordinances restricting algorithmic pricing in residential rentals, make clear that the regulatory landscape is evolving not just at the federal level but across dozens of jurisdictions simultaneously. Companies that operate in multiple states or that have any connection to the residential rental market face particular compliance complexity.

For companies operating in California, the Cartwright Act amendment applies across all industries and reaches the use of common pricing algorithms that employ competitor data, regardless of whether that data is publicly available. Companies using third-party pricing software that incorporates any form of competitor data should assess whether their use could be characterized as part of a "combination" or "conspiracy" to restrain trade.

---

41 *Gibson* at 1076 ("It would undoubtedly violate Section 1 were those competing hotels to agree among themselves to abide by a third party's pricing recommendations").

42 DOJ Guidance at 9-10.

43 DOJ Guidance at 5, 9, 12, 13.

V. CONCLUSION

Antitrust law governing algorithmic pricing remains in flux. The Ninth Circuit's *Gibson* decision provides meaningful clarity at the federal appellate level, drawing a distinction between independently adopted software licenses (not antitrust violations) and horizontal agreements among competitors to use common software and follow its recommendations (potentially per se unlawful). But the DOJ's continued interest in advancing broader theories of liability, the open question of how other federal courts will approach similar fact patterns, and the rapid expansion of state and local enforcement all counsel continued vigilance.

Across all these sources of legal authority, a coherent compliance framework has emerged. Companies must —

- preserve the independence of their pricing decisions;
- scrutinize the data inputs of third-party software;
- avoid communications with competitors about software adoption and use;
- integrate compliance into the technology evaluation process; and
- monitor an expanding patchwork of state and local regulations.

Companies that implement these practices — and that can demonstrate their implementation through documentation, training records, and ongoing monitoring — will be best positioned both to avoid liability and to demonstrate the hallmarks of an effective compliance program should they face government scrutiny.

The DOJ Guidance makes clear that the quality of a compliance program can affect how the government resolves an antitrust investigation, including whether it imposes court-mandated compliance requirements or external monitoring. In a rapidly evolving area of law, where the line between permissible use of pricing technology and anticompetitive coordination is still being drawn, proactive compliance is not merely good risk management — it is a prudent and necessary legal asset.