RAIL

The Journal of Robotics, Artificial Intelligence & Law

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@ meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

Ten Design Guidelines to Mitigate the Risk of AI Pricing Tool Noncompliance with the Federal Trade Commission Act, Sherman Act, and Colorado AI Act

Justin R. Donoho*

In this article, the author explains that companies increasingly face the risk of being targeted in lawsuits brought by governmental bodies and class action plaintiffs alleging unfair methods of competition in violation of the Federal Trade Commission (FTC) Act and agreements that restrain trade in violation of the federal Sherman Act. The author identifies recently emerging trends in such lawsuits, including one currently on appeal in the U.S. Court of Appeals for the Third Circuit and three pending in district courts, draws common threads, and discusses 10 guidelines that AI pricing tool designers should consider to mitigate the risk of noncompliance with the FTC Act, the Sherman Act, and Colorado AI Act.

"Express collusion violates antitrust law; tacit collusion does not. . . . [I]t is not a violation of antitrust law for a firm to raise its price, counting on its competitors to do likewise (but without any communication with them on the subject) and fearing the consequences if they do not."

—*In re Text Messaging Antitrust Litig.*,
782 F.3d 867, 872, 876 (7th Cir. 2015) (Posner, J.)
(case involving the Sherman Act)

While artificial intelligence (AI) pricing tools can improve revenues for retailers, suppliers, hotel operators, landlords, ride-hailing platforms, airlines, ticket distributors, and more, designers and deployers of such tools increasingly face the risk of being targeted in lawsuits brought by governmental bodies and class action plaintiffs alleging unfair methods of competition in violation of the

Federal Trade Commission (FTC) Act and agreements that restrain trade in violation of the federal Sherman Act.

This article identifies recently emerging trends in such lawsuits, including one currently on appeal in the U.S. Court of Appeals for the Third Circuit and three pending in district courts, draws common threads, and discusses nine guidelines that AI pricing tool designers should consider to mitigate the risk of noncompliance with the FTC Act and Sherman Act:

1. Stay tuned on *FTC v. Amazon* if considering allowing the algorithm to engage in tacit collusion;
2. Do not allow the algorithm to use shared nonpublic data to make individual price recommendations;
3. Do not allow the algorithm to publish customers' nonpublic information to other customers unless sufficiently nonsensitive, aggregated, and anonymized;
4. Stay tuned on the Third Circuit if considering allowing the algorithm to train with the benefit of information provided by each customer;
5. Maintain a procompetitive message to the market versus inviting a conspiracy;
6. Design and encourage pricing decision methods alternative to accepting the algorithm's recommended prices;
7. Train the algorithm with compliant pricing data;
8. Prevent algorithmic conspiracy; and
9. Audit use of the algorithm for noncompliance.

As a final guideline to mitigate the risk of noncompliance with the Colorado AI Act, this article recommends:

10. Add a human between the algorithm and consumers.

1. Stay Tuned on *FTC v. Amazon* if Considering Allowing the Algorithm to Engage in Tacit Collusion

In *FTC v. Amazon.com, Inc.*,[1] the FTC brought suit against a large online retailer alleging that its AI algorithm made unilateral price raises that it predicted other retailers would follow. According to the FTC, this activity, known as "tacit collusion,"

constituted "unfair methods of competition" in violation of the FTC Act although perfectly legal under the Sherman Act, as per this article's epigraph. The retailer moved to dismiss, arguing that unfair competition under the FTC Act requires an agreement, just like the Sherman Act requires an agreement. The FTC responded that the scope of the FTC Act reaches more broadly than the Sherman Act to cover tacit collusion by AI, thus pursuing its recently more aggressive stance regarding "unfair methods of competition" in the age of AI.[2]

The district court agreed with the FTC, finding that allegations of tacit collusion coupled with allegations of "anticompetitive intent or purpose" sufficed to state a claim for unfair competition under the FTC Act for purposes of Rule 12(b)(6).[3]

Fact discovery is proceeding, a bench trial is set for October 13, 2026, and appeals may follow. A final judgment may determine for the first time whether there exists any scope of prohibited unfair competition under the FTC Act beyond the prohibitions established by the Sherman Act. According to the retailer, the FTC cited "no case in which any district court has ever held a defendant liable on such a 'standalone' unfair method of competition claim."[4]

At stake in this heavyweight battle is the legality of a primary design choice for any AI pricing tool designer before starting to implement most or all of the design—whether to allow tacit collusion.

The remainder of this article provides guidelines to mitigate the risk of violating the Sherman Act, as well as the FTC Act, but only to the extent the FTC Act overlaps with the Sherman Act (or to the extent the AI pricing tool relies on Amazon's pricing data, see guideline 7). To the extent the FTC Act reaches beyond the Sherman Act regarding AI pricing tools, that is a new issue raised by *FTC v. Amazon,* so keep your eyes on it and factor it into your organization's risk management program if considering allowing the algorithm to engage in tacit collusion.

2. Do Not Allow the Algorithm to Use Shared Nonpublic Data to Make Individual Price Recommendations

Courts presiding over two AI pricing tool cases pending in district courts are drawing a bright line by prohibiting AI tools'

use of competitors' nonpublic information, as illustrated by the following two cases involving AI pricing tools where the AI pricing tool vendors' motions to dismiss were denied primarily on this basis. A key point for AI algorithm designers to note here is that although shared data cannot be used for any individual price recommendations, as illustrated in this section, that prohibition does not mean that the AI pricing tool cannot train with the benefit of information provided by each customer (a separate issue discussed in guideline 4).

In *In re RealPage, Inc., Rental Software Antitrust Litigation*,[5] tenants brought class actions against an AI tool vendor and its landlord customers, alleging that the vendor facilitated a price-fixing agreement by providing its customers price recommendations based on the customers' collective nonpublic "pricing and supply data," in violation of the Sherman Act. The vendor moved to dismiss, arguing that any competitor data a customer had access to was aggregated and anonymized. The district court ruled for the tenants, finding sufficient allegations nonetheless to allow the case to proceed to discovery due to the algorithm's use of "shared" nonpublic information in making its price recommendations. As the district court explained, the "most compelling evidence of horizontal agreement are allegations that [the landlord customers of the vendor] submitted real-time pricing and supply data to be compiled into a common algorithm, which was sent to all [other customers] as 'forward-looking, unit-specific pricing and supply recommendations based on their shared data' to achieve higher prices."

In *Duffy v. Yardi Sys., Inc.*,[6] tenants brought class actions against an AI tool vendor and its landlord customers, alleging that the vendor facilitated a price-fixing agreement by providing its customers price recommendations based on the customers' collective nonpublic "pricing, inventory, and market data," in violation of the Sherman Act—as in *In re RealPage*, but against a different AI tool vendor. Also as in *In re RealPage*, the district court held that the tenants plausibly alleged a conspiracy in violation of the Sherman Act and found the algorithm's use of nonpublic information compelling in this regard, stating: "Defendants would have the Court assume that the lessor defendants, having turned over their commercially-sensitive data and paid for the services [the AI tool vendor] offered, did not intend to use the information generated

as a result. . . . The Court finds that plaintiffs have plausibly alleged a conspiracy in violation of § 1 of the Sherman Act."

In sum, the Sherman Act prohibits AI pricing tools from using shared nonpublic data to make individual price recommendations.

3. Do Not Allow the Algorithm to Publish Customers' Nonpublic Information to Other Customers Unless Sufficiently Nonsensitive, Aggregated, and Anonymized

The Sherman Act prohibits AI pricing tools from publishing sensitive nonpublic data among its customers. Courts have upheld claims under the Sherman Act when competitors' nonpublic data were published to other competitors, unless the information was sufficiently nonsensitive, anonymized, and aggregated. For example, one court dismissed a Sherman Act claim involving exchange of anonymized and aggregated sales, production, and inventory data "(but never price data)."[7] By contrast, other courts have allowed Sherman Act claims to go forward where statistical reports provided "access to otherwise private information on the production and prices of other Defendants" and the ability to "reverse engineer the reports to identify which Defendant provided a given data set,"[8] or where competitors were permitted to exchange nonpublic employee compensation and budget data[9] or the "most recent price charged or quoted."[10]

4. Stay Tuned on the Third Circuit if Considering Allowing the Algorithm to Train with the Benefit of Information Provided by Each Customer

A case pending in the Third Circuit involving AI pricing tools dismissed claims involving not any exchange of nonpublic information or data pooling among customers but provision by each customer of "its current, non-public . . . pricing and [inventory] data to the [AI pricing tool] platform . . . the same third-party algorithm platform to which their co-defendants were submitting their own respective real-time and non-public pricing and [inventory] data."[11]

5. Maintain a Procompetitive Message to the Market Versus Inviting a Conspiracy

AI pricing tool vendors should typically refrain from emphasizing the tool's ability to raise prices, as courts have found the following alleged marketing strategies by AI pricing tool vendors, amounting to such, to be a "plus factor" and "invitation[] to collude" in finding plausible allegations that the vendor violated the Sherman Act: (1) "advertis[ing] its … software to [customers] as a means of increasing rates above those available in a competitive market,"[12] and (2) "educat[ing] clients on the pricing methodology and associated benefits of accepting all, or almost all [AI pricing tool] pricing recommendations, despite [decreasing sales]."[13]

On the other hand, advertising to customers their ability to raise prices through "surge" pricing recommended by the algorithm may avoid Sherman Act liability if, in the market for the customers' services being offered for sale, "There are from time to time an ever varying number of [customers selling their services], electronically flashing on and off like a laser beam [with r]arely … the same [seller] present at the same time or for the same length of time."[14]

While maintaining a procompetitive message is important for compliance, it will not render an otherwise noncompliant AI pricing tool compliant.[15]

6. Design and Encourage Pricing Decision Methods Alternative to Accepting the Algorithm's Recommended Prices

Courts have found AI tool vendors' failures to encourage the customer to enter or select alternative prices from those recommended by the algorithm another circumstance relevant to finding plausible allegations that an AI pricing tool vendor violated the Sherman Act.[16]

Thus, AI pricing tool vendors should build into their tools the ability for customers not only to accept the algorithm's recommended price but also ways for customers to implement alternative prices or pricing strategies. For example, the customer could be permitted the alternative of entering a specific numerical price of the customer's own choosing. As another example, if the algorithm is recommending a "price raising strategy" such as by implementing

price increases where the algorithm predicts competitors might follow those price increases, alternative options might include a "price undercutting strategy" to lower prices where the algorithm predicts sales will sufficiently increase to compensate for the lower price, or other strategies based on other metrics and algorithmic predictions.

Another option designers might consider offering customers is to train the algorithm with the customer's own pricing decisions as the customer selects any of the non-algorithmic options described in the prior paragraph. With sufficient such customer-specific training, algorithmically generated prices automatically accepted by the customer thereafter may sufficiently promote independent, customer-specific pricing decisions to avoid violating the Sherman Act.[17]

7. Train the Algorithm with Compliant Pricing Data

As Keith E. Sonderling, former Commissioner of the Equal Employment Opportunity Commission, once stated, "the reliability and lawfulness of the AI's output is only as good as the inputs."[18] That truism about lawfulness of an AI tool's outputs only if the inputs are lawful may not be limited to antidiscrimination laws and may also apply to antitrust laws. Specifically, just as using impermissibly biased training data as inputs to AI hiring tools risks noncompliance with antidiscrimination statutes,[19] using impermissibly fixed prices as inputs to train AI pricing tools risks noncompliance with antitrust statutes. For example, if an AI pricing tool were to train on the prices under dispute in *FTC v. Amazon* (see guideline 1) as the algorithm's inputs, the designer should consider whether the resulting outputs might prompt similar disputes.

8. Prevent Algorithmic Conspiracy

Ultimately, the AI pricing tool needs to be designed to act independently for each customer, not in concert for all customers. Thus, many guidelines in this article are focused on promoting algorithmic independence for each customer as opposed to promoting concerted action.

But the AI pricing tool should not be *so* independent that it reaches an agreement in restraint of trade all by itself.

This conundrum raises the question, can an AI ever truly reach an agreement all by itself, such that its designer or deployer might face liability resulting from a conspiracy originated by the algorithm?

While legal scholars have debated whether today's generation of AIs have legal capacity to agree,[20] one of today's leading AIs denies having the consciousness, intent, and understanding needed for genuine agreement.[21]

On the other hand, today's AIs are capable of negotiating the words in a written contract autonomously with other AIs and no human involvement.[22] Thus, courts presented with a written instrument created by such methods and appearing to be a contract might be inclined to apply the "four corners rule," which presumes that "an integrated, facially clear, and complete written agreement speaks for itself, without extrinsic evidence."[23] However, applying the four corners rule to such a contract presumes AI's capacity to form an agreement in the first place.[24]

Given the foregoing state of legal affairs and current state of AI, steps designers might take to prevent AI pricing tools from reaching price-fixing agreements on their own include the following: (1) do not allow the tool to negotiate express instruments that appear to be contracts, and (2) if AI ever becomes capable of forming the consciousness, intent, and understanding needed for genuine agreement, then add code to disallow the AI from forming any such price-fixing agreement.

9. Audit the Algorithm for Noncompliance

In *RealPage*, the district court found persuasive in denying dismissal of a Sherman Act claim a "regression analysis" performed by the plaintiffs that showed "a lessening correlation between … price and [inventory] after the start of [the alleged conspiracy]."[25]

Before that AI pricing tool found itself in that district court, it would have been a relatively straightforward addition for the designer to allow the tool to perform such an analysis, identify such a correlation, and produce warnings or change behaviors upon its detection. Whether via a "regression analysis" or more advanced data science techniques such as that offered by AI, AI tool designers

might consider building in such price-fixing agreement detection and warning systems as part of the design.

10. Add a Human Between the Algorithm and Consumers

AI tool vendors should consider requiring its customers to either enter their own prices or affirmatively approve every price recommended by the algorithm, in order for the customers to insert themselves between the algorithm and any consumers offered the price. That way, the AI tool vendors' customers might avoid being legally required to disclose the use of the AI tool to consumers, which may not be desirable for the customers. By contrast, if the AI tool vendors' customers automatically pass through the AI tool's price recommendations to its customers, modern AI statutes such as the Colorado AI Act may require disclosure to consumers.[26]

Summary

AI pricing tools designed to comply with antitrust and AI laws face fewer risks than those not designed for compliance, of an expensive class action lawsuit or government-initiated proceeding alleging violation of such laws. Moreover, by enabling and automating informed pricing decisions, AI pricing tools hold the potential to drive market efficiencies.

This article identified design guidelines to assist with such compliance and, relatedly, such market efficiencies, as follows:

1. Stay tuned on *FTC v. Amazon* if considering allowing the algorithm to engage in tacit collusion;
2. Do not allow the algorithm to use shared nonpublic data to make individual price recommendations;
3. Do not allow the algorithm to publish customers' non-public information to other customers unless sufficiently nonsensitive, aggregated, and anonymized;
4. Stay tuned on the Third Circuit if considering allowing the algorithm to train with the benefit of information provided by each customer;
5. Maintain a procompetitive message to the market versus inviting a conspiracy;

6. Design and encourage pricing decision methods alternative to accepting the algorithm's recommended prices;
7. Train the algorithm with compliant pricing data;
8. Prevent algorithmic conspiracy;
9. Audit use of the algorithm for noncompliance; and
10. Add a human between the algorithm and consumers.

Notes

* Justin R. Donoho is special counsel at Duane Morris LLP and a Certified Information Systems Security Professional. He may be contacted at jrdonoho@duanemorris.com.

1. FTC v. Amazon.com, Inc., 2024 WL 4448815 (W.D. Wash. Sept. 30, 2024).

2. FTC, et al., "Joint Statement on Competition in Generative AI Foundation Models and AI Products" (July 23, 2024) ("We are mindful of … the risk that algorithms can allow competitors to share competitively sensitive information, fix prices, or collude on other terms or business strategies in violation of our competition laws.… We will be vigilant of these and other risks that might emerge as AI technology develops further"); FTC, "Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act" (Nov. 10, 2022) (superseding prior one-page 2015 Policy Statement with 15-page detailed analysis and enumerating "practices that facilitate tacit coordination" as an example of unfair competition under the FTC Act); Former FTC Commissioner Terrell McSweeney, et al., "The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Antitrust Enforcement," 32 Antitrust 75, 76 (2017) ("the potential that pricing algorithms will facilitate tacit collusion beyond the reach of Section 1 of the Sherman Act is far from fanciful. Indeed, the Federal Trade Commission's authority under Section 5 of the FTC Act to prosecute 'unfair methods of competition' may be the only current tool available to police individual instances of algorithmic collusion").

3. FTC v. Amazon, 2024 WL 4448815, at **13-14.

4. Id., No. 23-cv-1495, ECF No. 178 at 8.

5. In re RealPage, Inc., Rental Software Antitrust Litigation, 709 F. Supp. 3d 478 (M.D. Tenn. Dec. 28, 2023).

6. Duffy v. Yardi Sys., Inc., 2024 WL 4980771 (W. D. Wash.).

7. Valspar Corp. v. E.I. Du Pont De Nemours & Co., 873 F.3d 185, 193 (3d Cir. 2017) (affirming dismissal of Sherman Act claim involving exchange of anonymized and aggregated sales, production, and inventory data "(but never price data)").

8. In re Turkey Antitrust Litigation, 642 F. Supp. 3d 711, 726-27 (N.D. Ill. 2022).

9. Todd v. Exxon Corp., 275 F.3d 191, 212 (2d Cir. 2001) (Sotomayor, J.)

10. United States v. Container Corp. of Am., 393 U.S. 333, 336 (1969).

11. Cornish-Adebiyi v. Caesars Ent., Inc., 2024 WL 4356188, at *2 (D.N.J. Sept. 30, 2024) (dismissing Sherman Act claim), on appeal, No. 24-3006 (3d Cir.) (oral argument tentatively scheduled for September 18, 2025). Compare Gibson v. Cendyn Grp., LLC, 2024 WL 2060260, at *6 (D. Nev. May 8, 2024) (dismissing Sherman Act claim involving a "'machine learning' theory—that the algorithms improved over time by running on confidential information provided by each [customer]. No [customer] gets direct access to the confidential information of another but gets the benefit of a system that has gotten better since it was launched … because it has run on the confidential data of many others in the past. In other words, the algorithms got better at predicting optimal … pricing with the benefit of information provided by each customer"), aff'd 2025 WL 2371948 (9th Cir. Aug. 15, 2025).

12. Duffy v. Yardi, 2024 WL 4980771, at **4-5.

13. In re RealPage, 709 F. Supp. 3d at 496, 509.

14. In re Meyer v. Uber Techs., Inc., No. 01-18-0002-1956 (AAA Feb. 22, 2020), available at No. 15-cv-9796, ECF No. 182-16, at 8 (S.D.N.Y. May 22, 2020) (on this basis distinguishing the classic "hub and spoke" conspiracy case of Interstate Circuit v. United States, 306 U.S. 208 (1939)). But see Meyer v. Kalanick, 174 F. Supp. 3d 817, 823 (S.D.N.Y. 2016) (before being superseded by the foregoing arbitral award in the same case, denying motion to dismiss under the authority of Interstate Circuit because the AI pricing tool provided customers an "assurance that all [customers] will charge the price set by [the AI pricing tool]").

15. See Olean Wholesale Grocery Coop., Inc. v. Agri Stats, Inc., No. 19 C 8318, 2020 WL 6134982, at **2, 5 (N.D. Ill. Oct. 19, 2020) (denying motion to dismiss Sherman Act claim against statistical reporting company that shared nonpublic information among competitors even though the company "is an intentionally secretive company" and marketed to customers only by "giving [its customers] the ability to improve their profitability").

16. In re RealPage, 709 F. Supp. 3d at 496, 509 (finding it circumstantial evidence of a conspiracy under the Sherman Act that the AI tool vendor "spen[t] considerable time … educat[ing] clients on the pricing methodology and associated benefits of accepting all, or all most all [AI pricing tool] pricing recommendations, despite [decreasing sales]"); Duffy v. Yardi, 2024 WL 4980771, at **4-5 (finding it a "plus factor" suggesting violation of the Sherman Act that "[the AI tool vendor]'s system works as advertised … only if each [customer] … adopts [a single recommended] price with very little, if any, second guessing").

17. See Duffy v. Yardi, 2024 WL 4980771, at *3 (explaining that ultimately the Sherman Act "applies only to concerted action that restrains trade: independent market decisions and conduct are not enough, even if there are parallels in timing or activities").

18. Keith E. Sonderling, et al., "The Promise and the Peril: Artificial Intelligence and Employment Discrimination," 77 U. Miami L. Rev. 1, 22 (2022).

19. See Justin R. Donoho, "Five Human Best Practices to Mitigate the Risk of AI Hiring Tool Noncompliance with Antidiscrimination Statutes," J. Robotics, AI & L. (July-August 2025).

20. See, e.g., Visa A.J. Kurki, A Theory of Legal Personhood at Chapter 6 ("The Legal Personhood of Artificial Intelligences") (Oxford 2019) (treating AIs acting as commercial actors along a spectrum from AI as a tool, to AI as a representative, to AI as a legal person); Claudio Novell, "Legal Personhood for the Integration of AI Systems in the Social Context: A Study Hypothesis," 38 AI & Society 1347, 1356 (2023) ("AIs are smart enough to act on the basis of reasons, trying to optimise the achievement of one or more goals, interacting with the external environment and being able to manipulate (also in a creative way) the received information as well as to implement new ones as perceived by the environment and by their own experience. In this sense, it seems possible to describe AIs as intelligent agents, capable of participating intentionally in relevant legal situations—e.g., contracts—without the ongoing supervision of the human principal"); Hon. Katherine B. Forrest (Fmr.), "The Ethics and Challenges of Legal Personhood for AI," 133 Yale. L. J. Forum 1175, 1209 (2024) ("Dobbs [v. Jackson Women's Health Org., 597 U.S. 215 (2022), overruling Roe v. Wade] eliminated a human developmental, cognitive, or situational awareness requirement for the bestowal of significant rights. It did this while diminishing the self-determination, and therefore right to personal liberty, of women. This framework could, ironically, be used to provide a basis for rights to a human creation—AI—as to which some believe there are moral and ethical responsibilities").

21. When your author asked CoPilot using GPT-4, "As an AI, do you think you are capable of having a meeting of the minds aka mutual assent with another AI or human," the AI responded, "No, I wouldn't be capable of achieving a true 'meeting of the minds' in the legal sense. Mutual assent requires the parties involved to understand and agree to the terms of a contract, with intentionality behind their consent. While I can process and analyze data, draft agreements, and even simulate negotiation-like behavior, I lack the consciousness, intent, and understanding needed for genuine agreement. My actions are based on patterns and programming, not conscious decision-making."

22. See, e.g., Ryan Browne, "An AI Just Negotiated a Contract for the First Time Ever—And No Human Was Involved," CNBC (Nov. 7, 2023), https://www.cnbc.com/2023/11/07/ai-negotiates-legal-contract-without-humans-involved-for-first-time.html.

23. Cheng v. Cont'l Classic Motors, Inc., 668 F. Supp. 3d 822, 828 (N.D. Ill. 2023).

24. Id. (explaining that courts apply the four corners rule on the theory that the contract's "explicit language stands for the intent of the parties").

25. In re RealPage, 709 F. Supp. 3d at 515.

26. See Colo. Rev. Stat. § 6-1-1704(1) ("a deployer or other developer that deploys, offers, sells, leases, licenses, gives, or otherwise makes available an artificial intelligence system that is intended to interact with consumers shall ensure the disclosure to each consumer who interacts with the artificial intelligence system that the consumer is interacting with an artificial intelligence system").