ALGORITHMIC PRICING AND TACIT COLLUSION IN DIGITAL MARKETS: THE DUAL ROLE OF DATA AND A COMPARATIVE ASSESSMENT OF GLOBAL AND INDIAN REGULATORY RESPONSES

Yashvi R. Mehta[*]

ABSTRACT

"Whether you use a smoke-filled room in a basement or you're using AI and an API, it's still the same thing. It's still collusion." -Jonathan Kanter

The rise of algorithmic pricing in digital markets has transformed the structure of price determination and challenged the conceptual foundations of traditional competition law. The paper begins by revising core antitrust doctrines and how digital markets challenge them. It then goes on to examine the mechanics of algorithmic pricing, tacit collusion, and how data concentration (symmetry and asymmetry) acts as a facilitator and barrier to tacit collusion. Unlike traditional cartels that rely on clear communication, algorithmic pricing systems often lead to tacit collusion through independent interactions, real-time data analysis, and self-learning methods that adjust pricing strategies without explicit agreement. This paper examines the growing issue of algorithmic tacit collusion, focusing on the dual role of data concentration. Against this backdrop, the paper also compares global regulatory responses, particularly of the European Union, the United States, and the United Kingdom, where authorities are actively addressing algorithmic tacit collusion, and against this backdrop, the paper critically evaluates India's stance on the same. It concludes by proposing targeted regulatory and legal reforms that aim to improve detection, ensure accountability, and shape policy, all while allowing innovation in data-driven markets.

Key Words: Digital Markets; Algorithmic Pricing; Tacit Collusion; Data Concentration; Competition Law; Enforcement Gaps; Regulatory Reforms.

[*] Yashvi R. Mehta is a third-year student of B.Com. LL.B. at the Institute of Law, Nirma University, Ahmedabad. The views stated in this paper are personal.

I. INTRODUCTION

Traditionally, antitrust enforcement has focused on the meeting of the minds as the essential point for legal action. However, we are now witnessing a change wherein the smoking gun, i.e. documents or communications that show a clear intent to restrain trade, such as coordinating prices with competitors instead of competing against them. is being replaced by an algorithm. In the past, laws were built around visible evidence of collusion, formal agreements, and smoke-filled rooms. With the rise of digital marketplaces, we have entered a time of silent coordination.

As companies increasingly use algorithmic pricing to manage their products and services, market interaction has shifted; it has moved from independent strategies to the collective optimization of Artificial Intelligence tools. In this new environment, the conspiratorial handshake has been replaced

by an algorithmic consensus, which creates a market where the lack of human interaction does not negate competition. This paper examines the intersection between algorithmic tacit collusion and the dual role of data concentration acting as a facilitator and as a barrier to tacit collusion, also arguing that current competition law frameworks inadequately capture the competitive harms arising from algorithmic pricing and tacit collusion.

The main issue lies in the well-established nature of tacit collusion facilitated by algorithmic pricing.[1] While tacit collusion has often been seen as a fragile and uncommon outcome, primarily due to issues such as human error or slow response times,[2] algorithms have effectively eliminated these issues. By monitoring market conditions and competitors in real time, and automating a practically "tit-for-tat" retaliation, algorithmic pricing can sustain supra-competitive prices without ever engaging in direct communication or agreement. This creates a gap where the outcome for the consumer is identical to that of a cartel, yet the behavior remains legally sound according to current standards that prioritize evidence of intent over economic effects.

Furthermore, it is argued that collusive stability isn't merely a byproduct of algorithmic pricing, but also of the structural environment created by data concentration.[3] The concentration of vast data sets in the hands of a few dominant players facilitates the "information symmetry" required for these

[1] OECD, 'Algorithms and Collusion: Background Note by the Secretariat' (OECD, 21–23 June 2017) <https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf> accessed 14 February 2026.
[2] Ariel Fzrachi & Maurice E Stucke, 'Sustainable and Unchallenged Algorithmic Tacit Collusion' (2020) 17 Nw J Tech & Intell Prop 217.
[3] Ron Jarmin and Amy O'Hara, 'Big Data and the Transformation of Public Policy Analysis' (2016) 35(3) *Journal of Policy Analysis and Management* 715.

algorithms to work with formidable perfection;[4] at the same time, this "information asymmetry" leads to data-based entry barriers where relatively nascent firms find it difficult to challenge collusion because they lack the data needed to train a competitive algorithm. As regulatory authorities begin to scrutinize robo-sellers,[5] the traditional boundaries of competition law are being pushed to their breaking point. This research aims to portray that, without a paradigm shift, i.e., moving away from intent-based "agreements" towards an effect-based analysis of the behavior of firms, the digital marketplace shall transform into a landscape of automated monopolies.

Traditionally, competition law has been designed to regulate competition among firms that compete primarily through price, output, and product quality. Market power has generally been assessed through factors like market share, the ability of the players to influence prices, and their control over supply.[6] Section 3 of the Competition Act, 2002,[7] reinforces the premise that the existing regulations have been designed to deal with human facilitation of collusion. However, the growth of digital markets has transformed how competition operates, challenging the adequacy of traditional competition laws in addressing modern market realities.

Digital markets are often organized around platform-based models that connect different user groups. These platforms benefit from network effects,

[4] Marco Gambaro, 'Big Data Competition and Market Power' (2018) 2 Mkt & Competition L Rev 99.
[5] Terrell McSweeny and Brian O'Dea, 'Implications of Algorithmic Pricing for Antitrust Enforcement' (*Federal Trade Commission*, 2017) https://www.ftc.gov/system/files/documents/public_statements/1286183/mcsweeny_and_odea_-_implications_of_algorithmic_pricing_antitrust_fall_2017_0.pdf accessed 06 February 2026.
[6] Raghuvansh Seth, 'Interplay of Algorithmic & Tacit Collusion with Competition Law' (2022) 16 NUALS LJ 131.
[7] Competition Act 2002, s 3.

wherein the value of their services increases as more users join. As a result, first-movers tend to consolidate their positions over time, making entry difficult for relatively newer competitors. Unlike traditional markets where competition can be sustained among several firms, digital markets often display a tendency towards dominance by a few players.

A central feature of competition in the digital markets is the role that data plays as a competitive asset. Firms collect and process vast amounts of data, which enables them to improve services, refine their algorithms, target advertising, and improve overall user experience. Over time, this accumulation of data creates a loop where better data improves services, improved services attract new users, and new users generate even more data. Smaller or relatively nascent firms lack access to comparable data sets, making it relatively difficult for them to garner market share, consequently acting as a barrier to entry and a potential source of market power.[8]

Many digital services are provided to consumers at little or no monetary cost; firms generate revenue through advertising or data monetization instead of charging their consumers directly. Consequently, even when services appear free, consumers may suffer through reduced innovation or diminished data privacy through market concentration. These developments complicate the assessment of anti-competitive conduct, particularly when competitive outcomes are influenced by automated technologies. When firms rely on algorithmic pricing to determine pricing and market strategies, the retaliation to competitors' pricing strategies becomes rapid, which raises concerns of coordination or anti-competitive outcomes emerging without explicit agreements, making regulation even more challenging.

[8] Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (OUP 2016).

The paper adopts a doctrinal and analytical research methodology based on statutory provisions, legal precedents, regulatory reports, and academic literature on competition law and digital markets. It examines Indian law alongside developments in the European Union and the United States to evaluate how regulators respond to algorithmic pricing and data-driven market power. Drawing from academic and policy sources, the study explores the challenges of algorithmic tacit collusion and data concentration. It also identifies gaps in legal and regulatory measures for addressing competition issues in digital markets. The analysis is guided by a consumer welfare framework, which assesses how changing market practices and regulatory actions affect consumer interests, market efficiency, and competition outcomes in digital markets.

II. THE DYNAMICS OF TACIT COLLUSION AND THE ALGORITHMIC CATALYS

Tacit collusion, often termed "conscious parallelism," represents a market state where independent firms achieve a supra-competitive price equilibrium without any formal agreement or direct communication.[9] Unlike explicit collusion, which relies on "smoke-filled rooms" and express communication, tacit collusion is a byproduct of rational, unilateral decision-making.

At its core, the phenomenon is driven by the realization of mutual interdependence, i.e., firms acknowledge that their individual profit-maximizing strategy is inextricably linked to the actions and reactions of their rivals, a principle recognized in cases like *Theatre Enterprises Inc. v.*

[9] OECD, Algorithms and Collusion: Competition Policy in the Digital Age (2017) <https://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm> accessed 09 February 2026.

Paramount Film Distributing Corp[10] in the United States and in the Indian *LPG Cartel case*[11] addressing parallel pricing.

The economic stability of this kind of arrangement is best explained through the lens of repeated games. In a static one-off interaction, the firms face the classic "prisoners' dilemma" wherein undercutting their rival to capture market share seems like the most plausible option; however, in a real-world market situation, the game is played indefinitely.[12] According to the Folk theorem, firms can sustain collusion only if they value future cooperative profits more than the immediate one-time gain of undercutting their competitor. This premise rests on a credible threat of retaliation. For instance, if Firm A drops its price (defects), Firm B must be able to detect this "cheating" and respond with a price drop of its own (punishment). If the punishment is swift and severe, the original defection becomes irrational, and a high-price equilibrium remains stable. Some market conditions are imperative for this equilibrium to hold, the first being "market transparency,"[13] i.e., firms must be able to observe each other's prices and sales volumes to distinguish between aggressive price cutting or a genuine decrease in demand.

The second is the "frequency of interaction,"[14] wherein the more often the firms interact, the shorter the "detection lag" shall be. The third is "product

[10] *Theatre Enterprises Inc v Paramount Film Distributing Corp* 346 US 537 [1954].
[11] *In Re LPG Cylinder Manufacturers* Case No 03/2011 (Competition Commission of India, 24 April 2012).
[12] Ann Nowé, Peter Vrancx and Yann-Michael Hauwere, 'Game Theory and Multi-Agent Reinforcement Learning' in Marco Wiering and Martijn van Otterlo (eds), Reinforcement Learning: State-of-the-Art (Springer-Verlag 2012) 441, 450.
[13] A Gupta, 'Algorithmic Collusion and its Challenges to Antitrust Regulations' (2025) *International Journal of Law Research & Analysis* https://www.ijlra.com/details/algorithmic-collusion-and-its-challenges-to-antitrust-regulations-by-arpita-gupta accessed 05 February 2026.
[14] S Assad and others, 'Algorithmic Pricing and Competition: Empirical Evidence from the German Retail Gasoline Market' (2024) 132(3) Journal of Political Economy 845.

homogeneity,"[15] i.e., coordination is simpler when the firms are selling identical goods rather than complex, differentiated products, where a price change might merely reflect a change in quality.

Despite these preconditions, human-led tacit collusion is seldom possible because humans are subject to cognitive biases and incomplete information.[16] For instance, an executive might misinterpret a competitor's logistical error as an intentional price cut, triggering a "price war." Furthermore, the sheer amount of data in modern markets often exceeds human processing capacity, making it difficult to monitor multiple rivals in real time. Historically, "frictions" like delays in detection, human error, and data overload served as a natural check against the emergence of tacit collusion between firms.

The advent of algorithmic pricing fundamentally alters the landscape by cancelling these human "frictions" which previously deterred tacit collusion. Algorithms do not collude in the human sense of intent, but they can achieve outcomes that mirror collusion, as a natural byproduct of profit maximization.[17] Algorithms can monitor thousands of competitor price points every second. This near-instantaneous surveillance eliminates the "detection lag." A firm might cheat weeks before being caught by a human, but, in an algorithmic system, retaliation occurs in milliseconds; by making punishment immediate, algorithms make the "deviation gain" negligible, thereby reinforcing the stability of the collusive equilibrium.

Beyond mere speed, modern reinforcement learning algorithms (such as Q-learning) can independently discover that supra-competitive pricing is the

[15] Louis Kaplow, Competition Policy and Price Fixing (Princeton University Press 2013).
[16] George J Stigler, 'A Theory of Oligopoly' (1964) 72(1) Journal of Political Economy 44.
[17] Emilio Calvano, Giacomo Calzolari, Vincenzo Denicolò and Sergio Pastorello, 'Artificial Intelligence, Algorithmic Pricing, and Collusion' (2020) 110(10) American Economic Review 3267.

most profitable long-term strategy. Experiments by Calvano et al.[18] (2020) demonstrated that AI agents, when left to maximize profits in a simulated oligopoly, naturally converge on collusive strategies that include reward-punishment schemes. These agents learn to "signal" intent through price movements and "punish" deviations without ever being programmed to cooperate. "*Relatively simple pricing algorithms systematically learn to play collusive strategies. The algorithms typically coordinate on prices that are somewhat below the monopoly level but substantially above the static Bertrand equilibrium. The algorithms learn these strategies purely by trial and error. They are not designed or instructed to collude, they do not communicate with one another, and they have no prior knowledge of the environment in which they operate."*[19]

The facilitation of tacit collusion can occur through a structural commonality, wherein multiple competitors may employ the same third-party pricing software (a "hub"), i.e., the underlying code acts as a centralizing force. Even if the firms never interact, the use of common logic or a similar data pool can act as a harmonizing agent.[20]

The *U.S. v. RealPage* case[21] represents a significant challenge from the DOJ against "algorithmic price-fixing." The DOJ claimed that landlords used a shared software "hub" to share sensitive data and raise rents together. The key legal issue is the shift from "independent judgment" to "collective delegation." The DOJ argued that outsourcing pricing to a common AI creates

[18] ibid.
[19] ibid.
[20] OECD, *Algorithmic Competition: OECD Competition Policy Roundtable Background Note* (2023) https://www.oecd.org/daf/competition/algorithmic-competition-2023.pdf accessed 08 February 2026.
[21] *United States and Plaintiffs v RealPage Inc*, No 1:24-cv-00710 (MDNC, filed 23 August 2024) (ongoing).

a de facto conspiracy, even without direct human contact. By showing that the software optimized for the revenue-to-occupancy ratio, favoring higher rents even if it led to more vacant units, the case aims to prove that algorithmic consensus is functionally and legally similar to a traditional price-fixing agreement.

Ultimately, the integration of algorithmic pricing makes tacit collusion a robust, high-speed market reality. By eliminating the detection lag and automating retaliation, algorithms remove traditional frictions that historically caused tacit collusion to fail.[22] This essentially results in a "perfected state" of conscious parallelism wherein firms achieve the supra-competitive profits of a traditional cartel through purely unilateral data-driven decisions. This evolution exposes a critical regulatory gap, as the resulting consumer harm occurs without the explicit "meeting of minds" required for a traditional antitrust prosecution.[23]

III. THE DUAL ROLE OF DATA IN FACILITATING AND CONSTRAINING TACIT COLLUSION

Data, in algorithmic pricing, plays a monumental role, yet its impact on market stability is governed by the structural distribution of that data. Data concentration, the gathering of vast datasets into the hands of a few dominant firms, operates as a double-edged sword, depending on whether such data is held by one dominant firm (asymmetry) or shared among a circle of elite incumbents (symmetry), which can act as a facilitator or a powerful barrier to tacit collusion resulting from algorithms. Understanding this tension is critical

[22] Ariel Ezrachi and Maurice E Stucke, '*Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*' (Harvard University Press 2016).
[23] (n 17)

to determining whether a market is trending toward monopolization or a stale supra-competitive oligopoly.

A. Data Asymmetry

In classical economic theory, the primary obstacle to any collusive arrangement is "noise," or uncertainty. When data concentration is asymmetric, i.e., it rests in the hands of a select few, or one firm, that its rivals cannot replicate, the very prerequisite of algorithmic data collusion, i.e., the symmetry of data for effective learning and decision-making, for the algorithm may reduce the feasibility of sustained tacit collusion.

Informational asymmetry introduces a fundamental misalignment in the market. For instance, if Firm A has access to real-time consumer data and a predictive demand analysis that Firm B lacks, Firm A then is no longer playing the same game as B and does not have to worry about any competition from B until it acquires the technology or booms.

In this scenario, Firm A (data-rich firm) has a lower incentive to participate in a tacit agreement. Coordinating with a relatively uncompetitive rival on a higher price, when one has a competitive advantage over the same, is an irrational decision. Moreover, superior datasets can be used to identify precisely where the rival is most vulnerable and effectively eclipse them within the market. Asymmetric data concentration allows the dominant firm to engage in limit pricing or hyper-personalized price discrimination, capturing the entire consumer surplus, consequently driving the rival out of the market. Therefore, data concentration can be used as a barrier to entry, ensuring that relatively nascent firms do not gain sufficient market intelligence to compete effectively.

Moreover, data asymmetry essentially destroys the signalling mechanism necessary for tacit collusion.[24] For instance, if Firm A's pricing logic is hidden behind a proprietary "black box" of exclusive data, here distinguishing between a strategic attack and a rational response to a private data signal is very difficult. This ambiguity causes the collusive structure to fail.

G. Data Symmetry

Conversely, when data concentration occurs symmetrically, with a small group of firms having access to the same data pools, the risk of tacit collusion increases exponentially. Symmetry acts as a facilitator for algorithmic coordination. When algorithms are fed relatively similar datasets, they are predisposed to reach the same outputs. The "uncertainty" that prevented humans from tacitly colluding is effectively eliminated, thus allowing for a level of price synchronization that is both independent in the eyes of law and "collusive" in its economic effect.

The EU Horizontal Cooperation Guidelines (2023)[25] specifically addresses this "data symmetry" in Chapter 6.[26] They view shared data pools and algorithmic pricing as key factors that can lead to collusion. The Guidelines caution that high-frequency data sharing, even through third-party platforms, can remove strategic uncertainty. This allows companies to reach a collusive equilibrium almost instantly. By removing the "detection lag," these digital systems promote synchronized market behavior similar to traditional cartels. To ensure compliance, the EU requires some technical safeguards.

---

[24] Marco Gambaro, 'Big Data Competition and Market Power' (2018) 2 Mkt & Competition L Rev 99.

[25] Commission, 'Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements' [2023] OJ C 259/1.

[26] ibid ch 6.

This keeps data as a means for innovation instead of a "glasshouse" for price coordination.

In a symmetric environment, the detection lag effectively drops to zero. When one firm's algorithm experiments with a price change, the other algorithm will respond to such a change by altering the price in milliseconds. This near-instantaneous feedback loop makes "cheating" on a collusive price floor impossible, as the retaliatory punishments are so swift that no short-term gain can be achieved from the defection.

Additionally, in a scenario where the firms use the same hub,[27] i.e., the same third-party algorithmic software for their pricing, the chances of collusion increase. This symmetry is often facilitated by data pooling or the reliance on a limited number of data sources. When firms use the same cloud-based data sources, they are essentially outsourcing their decision-making to a central logic, thus, virtually, creating a "hub and spokes" model[28], wherein even without the presence of a formal agreement, the concentration of symmetric data into these funnels ensures that the algorithms, systematically, "learn" to cooperate. They gradually, through trial and error, discover that in a transparent, symmetric market, the most profitable long-term strategy is to maintain high prices and punish any deviation instantly.[29]

In conclusion, the impact of data concentration on competition cannot be reduced to a single outcome; it is a dynamic force that dictates the stability of

[27] Bradley C Weber, 'Hub-and-Spoke Conspiracies: Can Big Data and Pricing Algorithms Form the Rim?' (2023) 26(1) *SMU Science and Technology Law Review* 4.
[28] Joseph E Harrington Jr, 'Hub-and-Spoke Collusion with a Third-Party Pricing Algorithm' (2025) CRESSE Working Paper https://www.cresse.info/wp-content/uploads/2025/09/2025_ps3_pa1_HARRINGTON-1.pdf accessed 09 February 2026.
[29] Leon Musolff, 'Algorithmic Pricing Facilitates Tacit Collusion: Evidence from E-Commerce' in *Proceedings of the 23rd ACM Conference on Economics and Computation (EC '22)* (ACM, 2022) 2 https://doi.org/10.1145/3490486.3538239 accessed 14 February 2026.

a market. Asymmetric concentration leads to monopolization by exclusion, while symmetric concentration leads to stagnation through automated collusion. In both these instances, current competition law, which focuses on explicit agreements and "mens rea," fails to capture the structural reality. Thus, data concentration serves a dual role: it provides the "intelligence" for algorithms to coordinate and the "fortress" to ensure that coordination remains unchallenged by market forces.

IV. GLOBAL REGULATORY RESPONSES

The rapid proliferation of algorithmic pricing has triggered a coordinated, albeit fragmented, global response. Antitrust authorities have shifted from mere observation to aggressive litigation and the introduction of ex-ante regulations.

In enforcement proceedings related to explicit collusion, the illegality of collusion depends on the existence of an agreement or a concerted practice[30]; therefore, authorities usually establish the presence of concerted practice or a "meeting of minds."

A. Regulatory Framework in the European Union

The application of Article101 of the TFEU[31] (Treaty on the Functioning of the European Union). The EU recognizes that tacit collusion is not *per se* unlawful.[32] Therefore, the first step to regulating tacit collusion would be to revisit the concept of "concerted practice." In the EU, Art. 101 of the TFEU[33] includes both agreements and concerted practices. A price-fixing agreement

[30] OECD, *Algorithms and Collusion: Background Note by the Secretariat* (n 12) 34.
[31] Treaty on the Functioning of the European Union [2016] OJ C 202/47, art 101.
[32] Whish and Bailey (n 47) 603.
[33] ibid.

essentially "centres around the existence of a concurrence of wills between at least two parties, the form in which it is manifested being unimportant so long as it constitutes the faithful expression of the parties' intention.[34]" In addition, a concerted practice is "a form of coordination between undertakings which, without having reached the stage where an agreement properly so-called has been concluded, knowingly substitutes practical cooperation between them for the risks of competition."[35] Moreover, in accordance with the EU Guidelines on horizontal cooperation,[36] agreement or concerted practice to exchanges of information between competitors (including pricing information) can be tackled under Art. 101 of the TFEU.[37]

H. Regulatory Framework in the United States

In the US, the concepts of agreement and concerted action are employed interchangeably, as constituting a "joint action," prohibited by §1 of the Sherman Act[38]. The term agreement or concerted action is not explicitly mentioned in the Sherman Act[39] it rather uses the terms "contract," "combination," or "conspiracy," and an agreement with an anti-competitive purpose encompasses all these concepts. In addition, the concepts of price fixing agreements and concerted action can be observed in the *Socony*[40] as well as the *Container Corp.*[41]

[34] Case T-41/96 *Bayer AG v Commission* [2000] ECR II-3383 [69].
[35] Case 48/69 *ICI v Commission* [1972] ECR 619 [64].
[36] Commission,'Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements' [2023] OJ C 259/1.
[37] ibid.
[38] Sherman Act 1890, s 1.
[39] Sherman Act 1890.
[40] *United States v Socony-Vacuum Oil Co*, 310 US 150 (1940).
[41] *United States v Container Corp of America*, 393 US 333 (1969).

Thus, in the US and the EU, the requisite for an agreement to be found is the concurrence of wills or the explicit "meeting of minds", and in the case of tacit collusion, this requirement remains unsatisfied.

In 2015, the Department of Justice **('DOJ')** gave a warning about the risks of algorithms for market consumers and authorities.[42] The 2024-2026 DOJ Statements on AI compliance,[43] released in late 2024 and enforced throughout 2025, codified the agency's stance on algorithmic collusion: "training a machine to collude is still collusion."[44] It integrated artificial intelligence into its enforcement priorities. These guidelines require firms to actively audit their AI systems for anticompetitive outputs, ensuring that "black box" algorithms do not inadvertently use "grim trigger" strategies or enable "surveillance pricing" by illegally collecting non-public data.

Notable enforcement actions, like the November 2025 RealPage settlement,[45] have drawn a clear line against using detailed, real-time competitor data to train revenue management models. This effectively imposes a 12-month "cooling-off" period on shared data to reintroduce the necessary delay in detection for a competitive market.[46]

---

[42] Ezrachi and Stucke (n 1) 39.

[43] United States Department of Justice, *Evaluation of Corporate Compliance Programs* (United States Department of Justice, September 2024) <https://www.justice.gov/criminal/criminal-fraud/page/file/937501/download> accessed 09 February 2026.

[44] Jonathan Kanter, 'Assistant Attorney General Jonathan Kanter Delivers Remarks at the 2024 Georgetown Law Global Antitrust Enforcement Symposium' (United States Department of Justice, 10 September 2024 <https://www.justice.gov/archives/opa/speech/assistant-attorney-general-jonathan-kanter-delivers-remarks-2024-georgetown-law-global> accessed 16 January 2026.

[45] *United States v RealPage, Inc* et al, No 1:24-cv-00710 (MDNC, Proposed Final Judgment, 2025).

[46] United States Department of Justice, *Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution* (Press Release, April 2015) <https://www.justice.gov/opa/pr/former-e-commerce-executive-charged-price-fixing-antitrust-divisions-first-online-marketplace> accessed 09 February 2026.

Although the case involved a simple pricing algorithm and a human agreement to collude, it still demonstrates that the DOJ is willing to pursue antitrust enforcement against pricing algorithms that facilitate collusive practices.

In addition, the DOJ has revived Section 2 of the Sherman Act,[47] Monopolization, shifting from traditional price-fixing investigations to addressing challenges against the monopolies facilitated by algorithms. This revival focuses on ecosystem foreclosure, where dominant firms use their control over proprietary training datasets, high-performance GPUs, and cloud computing to exclude emerging competitors. The debate has grown more intense throughout 2025. Enforcement officials are moving away from the "consumer welfare" focus and adopting a structural approach. This approach looks into whether vertical integration in AI creates situations that hinder the next wave of innovation. By using Section 2[48] to tackle the foreclosure of gatekeepers, the DOJ seeks to stop a "permanent digital oligopoly," where entering the market is blocked not by price, but by a huge informational and infrastructural gap.

More recently, in 2020, Deputy Assistant Attorney General Richard A. Powers said that "the U.S. legal standard for a criminal antitrust violation remains constant; it requires proof beyond a reasonable doubt of an agreement among two or more competitors to fix prices, rig bids, or allocate markets, that occurs in, or affects, interstate commerce. Criminal prosecution is typically limited to bid rigging, price fixing, and allocation agreements, and the Antitrust Division has significant experience prosecuting anticompetitive conspiracies carried out by a range of means and methods, which could include

[47] Sherman Act 1890, s 2
[48] ibid.

using pricing algorithms."[49] Powers further explained that in the context of collusive agreements, the U.S. will prosecute any involved intermediaries as well: "[I]f an intermediary, such as a programmer or platform, facilitates a conspiracy among competitors to use a common pricing algorithm for the purpose of fixing prices, under U.S. law, we could prosecute both the competitors and the intermediary who facilitated the illegal agreement."[50]

However, at the 21st Annual International Competition Network Conference in 2022, Assistant Attorney General Jonathan Kanter, who oversees DOJ's Antitrust Division, seemed to indicate that organizations might need to take proactive steps relating to algorithmic pricing. According to Kanter, "Whether you use a smoke-filled room in a basement or you're using AI and an API, it's still the same thing. It's still collusion." He suggested that there is a role for corporate compliance programs in preventing collusion by algorithms, and that companies proactively design and train algorithms and AI programs to avoid collusion, in a similar way to how they train employees to comply with other legal requirements[51].

I. Regulatory Framework in the United Kingdom

The UK's Digital Markets, Competition and Consumers **('DMCC')** Act[52], which took full effect on January 1, 2025, grants the Competition and Markets

[49] Richard A Powers, 'Deputy Assistant Attorney General Richard A Powers Delivers Remarks at Cartel Working Group Plenary: Big Data and Cartelization, 2020 International Competition Network Annual Conference' (*US Department of Justice*, 17 September 2020) <https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-powers-delivers-remarks-cartel-working-group> accessed 09 February 2026.
[50] ibid.
[51] , 'Competition Litigation Update – September 2023' (*Quinn Emanuel Urquhart & Sullivan LLP* September 2023) <https://www.quinnemanuel.com/the-firm/publications/artificial-intelligence-and-antitrust-when-do-algorithms-violate-competition-laws/> accessed 09 February 2026.
[52] Digital Markets, Competition and Consumers Act 2024 (UK).

Authority (**'CMA'**) the power to issue Pro-Competitive Interventions (**'PCIs'**). Unlike traditional lawsuits, PCIs allow the CMA to directly order firms to change their algorithms or data-sharing practices if they are found to be facilitating a "rigid" market equilibrium.

J. The Regulatory Framework In India

India's stance on algorithmic pricing was characterized by a period of cautious observation, where the Competition Commission of India **('CCI')** relied on a traditional intent-based interpretation of the Competition Act, 2002[53], wherein the prevailing legal philosophy necessitated a meeting of minds or an explicit agreement to establish a cartel violation, a standard that struggles to accommodate the nuances of algorithmic coordination.

Artificial Intelligence was largely viewed as a tool for efficiency rather than a vehicle for anti-competitive harm. The response to algorithmic pricing has transitioned from cautious observation to proactive regulation, specifically designed to bridge the accountability gap created by the proactive usage of Artificial Intelligence.

The *Samir Agarwal v. ANI Technologies*[54] (Ola-Uber case) serves as a definitive precedent for the Algorithmic Safe Harbor, where the CCI maintained a strict adherence to traditional evidentiary standards despite clear evidence of synchronized pricing. Here, it was alleged that the platforms facilitated a Hub-and Spoke conspiracy, arguing that the price-to-demand ratio was no longer being determined by independent drivers but by a centralized market algorithm that effectively fixed prices across the whole market. However, the CCI dismissed these allegations, reasoning the absence of a

[53] Competition Act 2002 (India).
[54] *Samir Agrawal v Competition Commission of India* (2020) 8 SCC 431.

"meeting of minds," the use of a common pricing algorithm did not constitute a horizontal agreement under Section 3 of the Competition Act, 2002[55]. It was concluded that the drivers were merely "accessories" to the platform's independent business model[56], effectively creating a loophole where centralized algorithmic coordination is treated as a unilateral efficiency rather than a collusive harm.

Recently, the CCI has shifted its focus toward the structural risks of data concentration and the "black box" of automated pricing, thus acknowledging that the traditional legal doctrines, founded on human agency, are insufficient for contemporary times.

1. THE 2025 MARKET STUDY

A definitive pivot occurred with the release of the CCI Market Study on Artificial Intelligence and Competition[57] (October 2025). This report acknowledged that AI- oriented algorithms could generate and sustain supra - competitive pricing without human intervention, and the phenomenon was labelled as "Algorithmic Coordinated Conduct." The study categorizes the risk into four distinct algorithmic types, which are "monitoring," "signaling," "self-learning," and a "hub and spokes model."

---

[55] Competition Act 2002 (India), s 3.

[56] FE News Desk, 'Ola, Uber under fire: Government probes "unfair" price discrimination between iPhone and Android users' *Financial Express* (23 January 2025) <https://www.financialexpress.com/trending/ola-uber-under-fire government-probes-unfair-price-discrimination-between-iphone-andandroidusers/3723917/> accessed 14 February 2026.

[57] Competition Commission of India, *Market Study on Artificial Intelligence and Competition* (Competition Commission of India, October 2025) <https://www.cci.gov.in/images/pressrelease/en/press-release1759756192.pdf> accessed 10 February 2026.

The CCI's findings suggest that in India's rapidly growing AI market, adoption is highest in sectors like retail, e-commerce, and logistics. This concentration has led the CCI to advocate for a preventive compliance model. Enterprises are now urged to conduct algorithmic self-audits, documenting their AI's design logic and data inputs to proactively identify "unintended coordination." This marks a departure from reactive enforcement.

2. THE DIGITAL COMPETITION BILL 2024

The proposed Digital Competition Bill, 2024, was a significant shift towards an ex-ante framework for the regulation of digital markets. ***Firstly,*** the bill does not apply to all entities; it is only focused on Systematically Significant Digital Enterprises **('SSDE's')**. A firm is designated as an SSDE only if it provides a core digital service and caters to at least ten thousand end users and a gross merchandise value of Sixteen Thousand cr. in India. By establishing these high quantitative thresholds, the bill aims to regulate only those "gatekeepers" whose size and data access allow them to distort the market ecosystem.

Secondly, Section 12 of the Bill, prohibits the SSDE's from using the non-public data of their users to compete. Furthermore, the Bill restricts cross-usage of data, preventing a conglomerate from merging user data from a messaging app with data from an e-commerce app to create an unbeatable predictive algorithm. By mandating data portability and interoperability, the DCB ensures that data remains a fluid asset rather than a tool for permanent market "lock-in."

Thirdly, Section 11 of the bill imposes a hard ban on self-preferencing, ensuring that the SSDE's search or ranking algorithm does not unfairly favor its own products or services over others. It also bans tying and bundling,

preventing a dominant firm from forcing users to accept a secondary service (like a payment gateway) as a condition for using the core platform. These *ex-ante* (proactive) obligations are designed to prevent "bottlenecking," where a dominant firm uses its control over one layer of the digital stack to monopolize another.

Fourthly, the penalty for global turnover is the most definitive aspect of the bill. Recognizing that small fines are often treated as a "cost of doing business" by tech giants, the bill introduces a penalty of upto 10% of their global turnover for non-compliance. Additionally, the Bill introduces the concept of Associate Digital Enterprises **('ADEs')**, ensuring that a parent company cannot bypass the law by delegating anti-competitive algorithmic behavior to a smaller subsidiary or a "shell" entity.

Also, the EU Digital Markets Act **('DMA')**[58] sets up a penalty structure that changes the risk-to-reward balance for digital platforms by shifting from responding to violations to preventing them. In contrast to traditional antitrust laws, which find it hard to show "intent" in complicated algorithms, the DMA hands down heavy financial penalties. Gatekeepers (In the context of the EU Digital Markets Act (**'DMA'**), Gatekeepers are large systemic digital platforms that act as intermediaries between businesses and consumers. They are not just big companies; they are identified by their ability to control entire digital ecosystems, such as app stores, search engines, or operating systems. Platforms like Apple, Meta, Microsoft, Amazon, etc. have been characterized as gatekeepers.) can face fines as high as 10% of their total global revenue for initial non-compliance. If they keep breaking the rules, that fine can increase

[58] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L 265/1.

to 20%. Additionally, the Commission can impose periodic fines of up to 5% of the average daily global revenue to encourage quick compliance.[59] Extreme measures, like forcing the sale of parts of the business, are also present, which create a tough environment where the cost of tacit collusion greatly exceeds any potential benefits from price-fixing. It effectively makes algorithmic transparency a required standard rather than an option.

Finally, the bill also moves the market from an intent-based to a compliance-based standard; in the older regime an intention to harm the competition had to be proven, under the bill, a mere violation of the same triggers a penalty. In addition, the SSDE carries the burden of proving it has adhered to the transparency and fairness mandates. This "presumptive" approach is specifically designed to solve the "Black Box" problem, forcing firms to make their algorithms auditable by design rather than hiding behind technical complexity.

The bill has faced significant criticism from industry stakeholders and legal experts. Critics argue that the transition to a rigid ex-ante regime could inadvertently stifle the very innovation it seeks to protect, creating a compliance -first culture that burdens domestic startups and misses the nuances of a rapidly evolving technological landscape.

The most prominent criticism is that the bill may act as a "success penalty" for growing firms. By designating companies as SSDEs primarily based on size and turnover, the law risks pulling domestic unicorns into a web of heavy-duty regulation too early. Industry bodies like IMAI have expressed concern[60]

[59] Grant Thornton, 'Digital Markets Act: An Overview of the New EU Regulation' *Grant Thornton* (Factsheet, 2025) https://www.grantthornton.ie/insights/factsheets/digital-markets-act-an-overview-of-the-new-eu-regulation/ accessed 10 February 2026.

[60] Kamya Pandey, 'IAMAI Continues to Oppose Ex-Ante Regulation in Its Comments on the Draft Digital Competition Bill' (*Medianama* 16 May 2024)

over the excessive discretionary power given to the Competition Commission of India (**'CCI'**) by the broad qualitative criteria for SSDE designation, which could possibly lead to arbitrary decision-making. This essentially creates a complex compliance mechanism where resources that could have been employed for R&D and scaling up are redirected toward avoiding presumptive legal violations. This could also possibly discourage venture capital investment in the tech sector[61].

Also, the regulation of large digital enterprises in India is currently carried out under a host of statutory regulations, the enforcement of which is vested with multiple regulators. These clashes between jurisdictions of authorities would impair the effective regulation of SSDE's. "For instance, the Draft DCB's provisions on data usage and portability may overlap with the recently enacted DPDPA. Data usage. While the Draft DCB focuses on the competition aspects, the DPDPA primarily concerns the processing of personal data. This potential overlap was recently examined in the CCI's WhatsApp privacy policy investigation, where WhatsApp challenged the CCI's jurisdiction to examine privacy-related matters. Both the Delhi High Court and Supreme Court allowed the CCI's investigation to proceed, distinguishing between privacy issues per se and their competition implications. Both courts clarified that while privacy matters fall under data protection law, the competition authority can examine how privacy policies affect market competition. This judicial precedent suggests how similar overlaps under the Draft DCB might

<https://www.medianama.com/2024/05/223-iamai-oppose-ex-ante-regulation-comments-draft-digital-competition-> accessed 10 February 2026.

[61] Internet Freedom Foundation, 'IFF's Submission on the Digital Competition Bill' *Internet Freedom Foundation* (2024) https://internetfreedom.in/iffs-submission-on-the-digital-competition bill/#:~:text=Inadequacies%20of%20the%20Digital%20Personal,to%20comply%20with%20a%20law accessed 10 February 2026.

be resolved, though regulatory uncertainty may persist for businesses navigating multiple compliance requirements.[62]"

V. ENFORCEMENT GAPS

The shift to autonomous pricing systems has exposed a profound enforcement gap in the current antitrust jurisprudence, which still remains anchored to the 20th-century economic assumptions. While traditional law is designed to punish the "meeting of minds," the speed and opacity of digital markets facilitate supra-competitive market outcomes that make gauging human intent difficult. This section explores the specific points of failure in the current legal framework that range from the fundamental challenge of defining an "agreement" in an era of machine learning to the evidentiary vacuum created by the "black box" algorithms. Also, the elimination of the "plus factors" used by regulators to prove collusion by specialized software. Ultimately, the rise of hyper-personalized pricing and hub-and-spoke software architectures creates a layer of digital camouflage that allows firms to extract total consumer surplus while remaining technically compliant with a legal code that was never intended to govern the "invisible hand" of an AI-driven market.

A. Agreement And the Posner Kaplow Debate

The prerequisite to establishing collusion is the presence of a contract, an agreement, or a "meeting of minds." However, in modern digital markets, achieving collusive outcomes without such explicit agreement becomes

[62] Anush Ganesh, Mohit Yadav and Gaurav Pathak, 'The Indian Draft Digital Competition Bill and Report: A Critical Perspective' (2025) 9(2) Indian Law Review 193 <https://doi.org/10.1080/24730580.2025.2506958> accessed 14 February 2026.

relatively easier. This has revived the debate between Posner and Kaplow[63] (two of the most influential legal scholars in antitrust history)

Posner argued for a pragmatic outcome-based definition of agreement. He posited that if an oligopolist raises its' prices with the expectation that its rivals will follow, and they do, the sequence could be deemed to be a unilateral contract. To Posner the meeting of minds is less important than the outcome of their actions[64].

Posner's view is tailor - made for contemporary times, for instance, if Bot A raises its prices and Bot B follows, Posner would argue that an agreement has been reached through the behavior itself.

Kaplow took a more formalistic view of the situation and argued that, for the law to be fair, it must punish a specific act and not just a market condition[65]. For instance, if Firm A raises prices and Firm B follows, they essentially have "observed the world" and not tacitly colluded.

The problem with Kaplow's view is that it creates a safe harbor for algorithms. If two bots arrive at the same price because of their individual reward functions, both have independently discovered that high prices are better than price wars, and there has been no "communicative act." Under this

[63] Lewis Kornhauser, 'The Economic Analysis of Law' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Spring, 2022 Edition) <https://plato.stanford.edu/archives/spr2022/entries/legal-econanalysis/> accessed 14 February 2026.
[64] Richard A Posner, 'Book Review (reviewing Louis Kaplow, *Competition Policy and Price Fixing* (2013))' (2014) 79(3) *Antitrust Law Journal* 761.
[65] Martha T McCluskey and others, 'Law and Economics: Contemporary Approaches' (2016) 35(1) Yale Law & Policy Review 297 http://www.jstor.org/stable/26601712 accessed 10 February 2026.

logic, which also mirrors some Supreme Court precedents like Twombly, this is "conscious parallelism," which is perfectly legal.

The enforcement gap exists because the law currently follows Kaplow, but the market is behaving exactly like Posner feared. We have reached a point where algorithms can inflict 100% of the harm of a cartel, while maintaining the technical innocence of independent actors.

B. The Liability Gap and The "Black Box Problem"

The transition to autonomous algorithmic systems has introduced a profound liability gap that threatens the foundational principles of corporate accountability. At the center of this gap is the "Black-Box" Problem, i.e., modern pricing systems often use deep reinforcement learning models whose decision-making processes are non-linear and opaque. Even the developers who program the same cannot always trace the specific logic that led the algorithm to adopt a collusive price point over a competitive one; this severs the traditional legal link between conduct and intent. When an algorithm finds that the "supra competitive pricing" is the mathematically optimal path to profit- maximization, it does so without human intervention, creating a scenario where harmful market outcomes emerge in a vacuum of human culpability.

This autonomy creates a secondary challenge regarding the legal status of the algorithm versus the firm that employs it. Traditionally, the principal is responsible for the agent's acts, here algorithms are increasingly acting beyond their original instructions, evolving strategies that their creator may not have foreseen or desired. This raises a critical question: Should firms be held to a standard of Strict Liability for any anti-competitive outcome

produced by their software, or does the "Black Box" nature of the technology provide a defense?

Holding companies liable for autonomous machine behavior risks punishing firms for unintended practices, while failing to hold them liable creates a shield of ignorance, which encourages companies to outsource potentially illegal practices to a black box.

The EU AI Act[66] introduces a risk-based regulatory framework that fundamentally alters the black-box defense in antitrust law. Mandating transparency and human oversight for specific systems, it creates accountability, which can be used to prove collusion. It categorizes AI systems into specific tiers with escalating transparency obligations. According to Articles 12 and 13[67], the High-Risk and General-Purpose AI tiers are legally required to maintain automatically generated logs and comprehensive legal documentation for at least ten years. By shifting accountability from a voluntary choice to a legal mandate, the act ensures that any system having the capability to influence market dynamics is traceable and accountable. This allows regulators to bypass the struggle of proving human intent, thus focusing on whether AI was allowed to reach a collusive equilibrium.

In the Eturas case[68], it was established that awareness of a collusive system can be enough to trigger liability; these cases still involved a human nexus. In a purely algorithmic market, where bots "signal" to each other through micro-fluctuations in price, there is no human awareness. As of today, regulators are

[66] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2021] OJ C 65/1.
[67] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2021] OJ C 65/1, arts 12–13.
[68] Case C-74/14 *Eturas UAB and Others v Lietuvos Respublikos konkurencijos taryba* EU:C:2016:42, [2016] 5 CMLR 13.

contemplating whether to introduce a "Liability by design" mandate, which would require companies to ensure that their algorithms are aware of the compliance.

C. The Plus Factors Gap

When the evidence of explicit agreement is absent, the court considers "plus factors," i.e., behaviors that would be economically irrational unless the firms were conspiring. For instance, if Firm A raises prices when demands are falling, it becomes a plus factor as it contradicts the logic of independent competition. Algorithms have effectively killed this standard of proof.

Pricing bots are designed to maximize profit by observing the market at high frequencies. A bot realizes that a price war is a negative-sum game. If it lowers prices to capture market share, a rival's bot will notice the change in milliseconds and match it. This reaction cancels out any gain and results in lower profits for both companies. As a result, the bot recognizes that keeping prices high is the only sensible choice. In a courtroom, this leads to a Plus Factors Gap. The absence of price competition is no longer seen as "irrational behavior" signaling a conspiracy. Instead, it becomes the most logical and sensible action for a machine. By making collusion the most rational choice for an independent actor, algorithms eliminate the evidence that regulators previously relied on to prove a crime.

D. The Pricing-As-A-Service (Paas) Model

The biggest structural issue in 2026 is the growth of Pricing-as-a-Service (PaaS). Instead of creating their own unique bots, entire industries from real estate to hospitality now subscribe to the same third-party software platform, like RealPage or Cendyn. Here, the software provider gathers non-public,

sensitive data from all competitors and uses a single algorithm to provide pricing recommendations for everyone[69]. Typically, a hub-and-spoke conspiracy needs evidence that the competitors knew they were using the same hub to set prices. Companies can still argue they were just using a productivity tool and were unaware of their competitors' actions, as shown in the 2025 RealPage settlement.[70] Regulators are now trying to prove that the algorithm itself serves as the facilitator. However, current laws still struggle to hold the "spokes" accountable if they merely clicked accept on a machine-generated suggestion.

Ultimately, the enforcement gaps identified across these five dimensions reveal a fundamental misalignment between 20th-century legal standards and 21st-century technological realities. The transition from human-led cartels to autonomous pricing systems has effectively decoupled market harm from legal culpability. By exploiting the "Posner-Kaplow debate's" focus on explicit communication, algorithms have created a "safe harbor" for non-competitive outcomes that mirror the effects of a monopoly while maintaining the technical innocence of "independent" action. The erosion of "Plus Factors" and the emergence of the "Black Box liability gap" further insulate firms, allowing them to outsource their pricing strategies to unreachable code that operates beyond the reach of "intent-based" laws. Furthermore, the structural shift toward "Hub-and-Spoke" software models has centralized market power in the hands of third-party vendors, creating a "rimless" coordination that current jurisprudence is ill-equipped to prosecute. Collectively, these gaps

[69] Anshika Tyagi, 'Hub and Spokes Cartel' (2023) 6 Int'l JL Mgmt & Human 860.
[70] US Department of Justice, 'Justice Department Requires RealPage to End the Sharing of Competitively Sensitive Information and Alignment of Pricing Among Competitors' (*Department of Justice*, 24 November 2025) https://www.justice.gov/opa/pr/justice-department-requires-realpage-end-sharing-competitively-sensitive-information-and accessed 10 February 2026.

demonstrate that the traditional "handshake" standard of evidence is increasingly obsolete; without a radical reimagining of the notion of an "agreement" and a shift toward accountability for algorithmic outcomes rather than intentions, the digital economy will continue to move toward a state of stable, high-price synchronization that remains invisible to the law.

VI. REFORMS AND RECOMMENDATIONS

Digital markets require a regulatory shift from punishment to proactive oversight. As autonomous agents render traditional enforcement tools obsolete, a new regulatory framework is required, a model that focuses on ex ante regulation and emphasizes consumer welfare and structural efficiency. The following recommendations provide a roadmap for effective navigation and regulation of digital markets.

A. Systematic Investigation and the "Red Zone Mapping"

Academic consensus suggests that the nature of antitrust enforcement should evolve from a passive and reactive model to an active and preventative one. This would begin with a systematic market study designed to map the digital economy's high-risk zones.

Sectors with high algorithmic densities should be prioritized, for instance markets where over 60% transactions are executed via automated agents should be kept under the radar, since these markets would naturally have adverse effects on competition.

Drawing on the 2025 OECD Guidelines[71], sector-specific enquiries should focus on "essential consumer markets" like housing, energy, or travel. These

[71] OECD, *OECD Principles on Artificial Intelligence* (OECD Publishing, 2025).

enquiries are designed to identify points, i.e., specific data streams all algorithms use to coordinate.

B. Strategic Data Asymmetry

Regulators should mandate the introduction of noise or delayed feeding of data within "red- zone" sectors. Requiring algorithms to operate with slightly varied data or delayed signals can disrupt the symmetry necessary for tacit collusion, thereby restoring the competitive friction that automated systems tend to remove. It serves as a sophisticated regulatory intervention designed to disrupt the perfect transparency of data that catalyzes tacit collusion.

When all pricing bots access the same high-frequency data streams at the same time, they reach a stable point where any effort to compete on price is quickly noticed and stopped. This makes cutting prices mathematically pointless. By forcing a delay on how fast a firm's price change is sent to its rivals' APIs, regulators create a window of uncertainty. This short informational gap brings back the classic reason for a firm to lower prices, as it lets them gain significant market share before a competitor's bot can see and match the change. In the end, strategic differences change the market from a scenario of complete transparency to a competitive fog, bringing back the friction and risk needed to stop automated agents from settling on a permanent, high price level.

C. Algorithmic Sandboxing

Algorithmic sandboxing is the practice of isolating an algorithm within a restricted environment. It requires pre-market safety certification for a high-impact pricing software. Here, the firms in "red zone" sectors would be required to test their pricing algorithms in a regulatory sandbox, where it

would be monitored by state-sponsored watchdog AI to observe how it interacts with other market participants.

If the sandbox indicates that the bot naturally finds that the best strategy is to stop competing and keep a high-price balance, the software will not receive a license for deployment until its reward digital cartel function is re-coded to focus on volume and active competition. This approach makes technology more human-like by ensuring that competitive values are incorporated into the code's design, rather than relying on a bot created for profit maximization to unintentionally uphold fair market principles.

The UK Financial Conduct Authority **('FCA')** Regulatory Sandbox[72] evolving into a "Supercharged" AI-focused model by 2026. It uses a proactive Safe Space approach that shifts the focus from punishing firms after the fact to preventing issues before they occur. By giving firms, a controlled setting to test automated pricing models with synthetic datasets and cloud-based Algorithmic Surveillance tools, the sandbox lets regulators observe the pricing system before it is scaled. This framework helps solve the detection lag by allowing the FCA to spot collusive tendencies in real-time. Thus, this model changes algorithmic auditability from a legal obstacle into a necessary step for entering the market.

D. Mandatory Audit Trails:

One of the most dehumanizing aspects of algorithmic pricing is the "Black Box" problem, which means that a price can change a thousand times a day, and no one knows why. To restore the rule of law, we must require Searchable

[72] Financial Conduct Authority, *Regulatory Sandbox Guide* (Updated 2025) <https://www.fca.org.uk/publications/whatever-the-actual-url-is> accessed 10 February 2026.

Audit Trails. This requirement acts as a "flight recorder" for the economy. Every time an algorithm changes a price, it must log the specific data inputs it used, the competitive signals it detected, and the specific goal it was trying to achieve at that moment.

These logs must be unchangeable and available to regulators. By creating a digital record of decision-making, the black box is eliminated. An audit trail ensures that if a market failure happens, people can trace the decision back to a specific developer or corporate goal. This restores accountability to the human creators behind the code, making sure that the "efficiency" of an algorithm never serves as an excuse for avoiding corporate responsibility.

K. Establishing Strict Liability for Hubs

The rise of "Pricing-as-a-Service" **('PaaS')** has led to a new, decentralized form of collusion where the "Hub" software provider acts as the brain for an entire industry. Under current law, the "spokes" (the competitors) often claim they were just buying a tool, and the "hub" claims it is just a neutral platform. To bridge this gap, we need Strict Hub-and-Spoke Liability. This reform suggests that if a vendor markets an algorithm that uses pooled, non-public data from multiple competitors to recommend prices, that vendor is no longer a "service provider"; they are a Cartel Facilitator.

Humanizing this reform means recognizing that "shared software" is the modern equivalent of a "smoke-filled room." Any firm that subscribes to a hub, knowing that its direct rivals are also using that hub's optimization logic, should be legally presumed to have joined a horizontal agreement. This prevents the outsourcing of collusion and ensures that the law keeps pace with the structural changes of the digital economy. It holds both the software creator

and the corporate user responsible for the harm caused by a synchronized market.

L. Shifting The Burden of Proof

The biggest challenge in modern antitrust is the "intent-centric" model. Regulators need to show that someone intended to fix prices. In machine learning, this is a lost cause because the bot's "intent" is just a mathematical function aimed at maximizing reward. Scholars from Cambridge suggest we should adopt a Rebuttable Presumption of Concerted Practice. With this change, if a market run by algorithms shows sustained, high prices like those of a traditional cartel, the law won't ask regulators to find definitive proof, like a "smoking gun" email. Instead, the responsibility shifts to the company.

The firm must "humanize" its AI by clearly explaining, in simple terms, how its bot reached those price points using legitimate competitive logic, such as reacting to supply changes, instead of relying on learned patterns of silent cooperation with competitors. This change acknowledges that companies have a "duty of care" to the market. If they decide to introduce a "black box" into the economy, they must justify its actions. This ends the time when corporations could hide behind "machine autonomy" and reap the benefits of a digital cartel.

VII. CONCLUSION

The shift from human-run cartels to automated, data-driven pricing models represents a major change in the history of antitrust law. This paper has shown that algorithmic pricing is not simply a neutral tool for efficiency; it is a complex system that can deeply change competition by substituting the market's "invisible hand" with a self-learning "invisible code." By examining

data symmetry and high-frequency interactions, we observed how modern pricing bots can create stable, above-market outcomes, leading to tacit collusion, without requiring human agreements or formal discussions. In this new digital landscape, the old legal standard of an "agreement" has become problematic. It allows companies to enjoy the benefits of a cartel while claiming to act "independently."

The analysis of current enforcement gaps shows that the law is losing to the algorithm. Companies are taking advantage of the Posner-Kaplow stalemate. They delegate decision-making to "Black Box" models and eliminate the "Plus Factors" that regulators once used to identify conspiracy. This creates a barrier against liability. The growth of the Hub-and-Spoke model through third-party software has further concentrated market power. This setup lets entire industries coordinate their actions using a shared "digital brain." The ongoing crises in areas like rental housing and global logistics demonstrate that these arrangements pose a serious threat to the consumer's role in the economy. By moving toward a regulatory regime defined by Algorithmic Sandboxing, Mandatory Audit Trails, and the Inversion of the Burden of Proof, we can remove the masking of machine autonomy. These reforms require that companies take full responsibility for their "digital employees." If a bot learns to collude, its creators should face strict liability. We need to shift from a reactive, intent-based legal system to a proactive, outcome-based approach that treats market fairness as a necessary part of the digital age.

Ultimately, the goal of antitrust is not to block technological progress. Instead, it is to ensure technology benefits everyone, not just the interests of a few. Maintaining a fair, competitive marketplace means recognizing that while algorithms make choices, humans must remain accountable. By closing

enforcement gaps and implementing the reforms suggested in this study, we can make sure the "Digital Eye" of the algorithm monitors the market for the consumer's benefit, not for exploitation.