CIRANO
Knowledge into action

ALGORITHMIC PRICING AND COMPETITION: BALANCING EFFICIENCY AND CONSUMER WELFARE

FRÉDÉRIC MARTY
THIERRY WARIN

PR
2025PR-09
FOR REFLECTION

CIRANO

Knowledge into action

ISSN 2563-7266 (online version)

Algorithmic Pricing and Competition: Balancing Efficiency and Consumer Welfare[1]

Frédéric Marty, PhD
Ancien membre du Collège de l'Autorité de la concurrence française au titre de personnalité qualifiée pour les professions réglementées
CNRS – GREDEG – Université Côte d'Azur
CIRANO

Thierry Warin, PhD
HEC Montréal
CIRANO

2025-08-04

Pour citer ce document / To quote this document

Marty, F., & Warin, T. (2025). Algorithmic Pricing and Competition: Balancing Efficiency and Consumer Welfare (2025PR-09, Pour réflexion, CIRANO.) https://doi.org/10.54932/TXGO9604

JEL Classification: L41; D43; L13; K21; G18

---

[1] Note préparée dans le cadre de la consultation du Bureau canadien de la concurrence du 4 août 2025.

Abstract

This article examines the competitive implications of algorithmic pricing in digital markets. While algorithmic pricing can enhance market efficiency through real-time adjustments, personalized offers, and inventory optimization, it also raises substantial risks, including tacit collusion, discriminatory pricing, market segmentation, and exploitative consumer manipulation. Drawing on theoretical models, simulations, and emerging empirical evidence, the brief explores how algorithmic strategies may lead to supra-competitive prices without explicit coordination, particularly in oligopolistic or data-rich environments. It also highlights how common algorithm providers, shared data sources, and learning dynamics can undermine competition. Special attention is given to the challenges posed by loyalty penalties, ecosystem lock-in, and granular predatory pricing. The paper concludes with a set of policy recommendations emphasizing updated enforcement tools, transparency mechanisms, ex ante regulation for dominant platforms, and a coordinated approach to digital market oversight that balances innovation with consumer protection.

Résumé

Cet article examine les implications concurrentielles de la tarification algorithmique sur les marchés numériques. Si la tarification algorithmique peut améliorer l'efficacité du marché grâce à des ajustements en temps réel, des offres personnalisées et une optimisation des stocks, elle présente également des risques importants, notamment la collusion tacite, la tarification discriminatoire, la segmentation du marché et la manipulation abusive des consommateurs. S'appuyant sur des modèles théoriques, des simulations et des données empiriques émergentes, cet article explore comment les stratégies algorithmiques peuvent conduire à des prix supraconcurrentiels sans coordination explicite, en particulier dans les environnements oligopolistiques ou riches en données. Il souligne également comment les fournisseurs d'algorithmes communs, les sources de données partagées et la dynamique d'apprentissage peuvent nuire à la concurrence. Une attention particulière est accordée aux défis posés par les pénalités de fidélité, le verrouillage de l'écosystème et les prix prédateurs granulaires. L'article conclut par un ensemble de recommandations politiques mettant l'accent sur la mise à jour des outils d'application, les mécanismes de transparence, la réglementation ex ante des plateformes dominantes et une approche coordonnée de la surveillance du marché numérique qui concilie innovation et protection des consommateurs.

1. Introduction

Algorithmic pricing (often driven by AI) is increasingly used to set prices in real time across online markets. Competition authorities recognize it can promote competition through innovation and efficiency gains, but also harm competition via collusion, discrimination, and manipulation. Pricing algorithms rapidly process vast data (on demand, rivals' prices, consumer behavior) and adjust prices faster than any human, yielding pro-competitive benefits like dynamic supply-demand matching, better inventory management, and even helping new entrants target niche segments. At the same time, regulators worry that algorithms confer new forms of market power and consumer harm. Key concerns include tacit price coordination sustaining supra-competitive prices without explicit collusion, the development of parallel prices patterns resulting from decentralized and autonomous decisions but based on converging algorithmic recommendations, unfair personalized pricing that exploits certain consumers, and manipulative tactics leveraging consumer data. These risks are not just theoretical – real-world cases have shown algorithms producing collusive-like outcomes and exploitative pricing strategies. This report examines critical dimensions of algorithmic pricing, weighing efficiency gains against risks to competition, and outlining possible policy responses.

2. Efficiency vs. Consumer Welfare: Redistributive Effects

A core issue is the tension between **total welfare (market efficiency)** and **consumer welfare** under algorithmic pricing. Advanced pricing algorithms let firms finely segment customers and even approach *first-degree price discrimination* – charging each buyer the maximum they are willing to pay. In theory, a monopolist using perfect personalized pricing would eliminate deadweight loss (selling to every consumer who values the product above cost), thus maximizing total economic welfare. However, virtually all consumer surplus is captured by the seller, leaving consumers worse off than under simpler pricing. The U.S. Department of Justice has similarly observed that while perfect price discrimination can be allocatively efficient, it allows a monopolist to extract all consumer surplus, harming consumers despite higher output. In competitive markets, personalized pricing might benefit some consumers – for example, if rivals undercut each other with targeted discounts to win price-sensitive shoppers. A new entrant could use personalized coupons to lure loyal customers away from an incumbent, which increases those customers' welfare and promotes competition. But when competition is weak (e.g. a dominant platform or an oligopoly adapting in parallel), personalization will likely harm consumers overall. Loyal or high-value customers end up paying higher prices, while only the most price-sensitive shoppers see discounts – a phenomenon known as the "loyalty penalty." Studies in telecom and insurance markets have shown long-time customers often face steadily rising rates, whereas new or switching customers get cheaper deals. Algorithms make such strategies easier to execute at scale, identifying which customers are unlikely to switch and quietly charging them more, while funneling discounts to those who shop around. These outcomes pit allocative efficiency against equity and consumer protection. Traditional competition law focuses on consumer welfare (prices, output, quality), so if algorithmic pricing increases total efficiency but also creates significant consumer harm, enforcers may need to consider intervention on distributive grounds.

Algorithm-driven personalization can also be opaque[2], raising fairness-related concerns[3]. Some experts argue firms have a “digital responsibility” to ensure their pricing algorithms are fair and not unduly exploitative. In a fully automated “man-out-of-the-loop” pricing scenario, oversight mechanisms or audits might be needed so that algorithms do not systematically prey on certain consumer groups. Regulators could, for example, require periodic audits of algorithmic outcomes to detect biases or patterns of exploiting loyal customers, analogous to fairness checks applied to AI in credit or hiring decisions. (Notably, a New York State law now requires online sellers to disclose when prices are personalized for an individual, to alert consumers and discourage covert discrimination.) Imposing such fairness checks on pricing algorithms involves trade-offs in innovation and business autonomy, but it underscores that maximizing total welfare is not the same as maximizing consumer welfare. The case of near-perfect price discrimination shows that algorithms can make markets more efficient yet substantially worse for consumers. Competition authorities may need to clarify their objectives – is the mandate purely to ensure efficient markets, or also to prevent extreme surplus transfers that undermine consumer welfare? This question underlies many of the issues discussed below, including how far to go in guiding or regulating algorithmic pricing practices.

3. Risks of Tacit Collusion and Supra-Competitive Prices

[2] Two distinct forms of opacity can be identified in algorithmic pricing systems. The first is **natural opacity**, which arises from the inherent complexity of dynamic and personalized pricing mechanisms, particularly when driven by algorithmic processes and artificial intelligence. This includes, for instance, trade-offs between exploration and exploitation strategies in algorithmic decision-making. The second is **constructed opacity**, which is deliberately engineered—potentially to hinder effective regulatory oversight of pricing practices, but more critically, to reduce the comparability of offers from the perspective of consumers.

[3] The redistributive effects stemming from a firm’s pricing decisions may be examined from a competition law perspective through two distinct analytical lenses. First, the extraction of a significant share of consumer surplus represents a paradigmatic manifestation of monopoly power, particularly where such a position is insulated by substantial barriers to entry. Second, the implementation of discriminatory pricing conditions may be viewed as the exploitation of an informational advantage over consumers—one that arises from their compelled consent to the use of personal data as a prerequisite for accessing a service. In the absence of viable market alternatives—whether due to a lack of competition or to ecosystem-based lock-in—the user of a digital service is left with no meaningful choice but to accept such terms. The platform’s capacity for surplus extraction in such a context reflects not profit in the classical sense (as a reward for past investment), but economic rent derived from its control over data enabling differential treatment.

A prominent concern is that pricing algorithms could facilitate collusive outcomes (Marty et Warin, 2023a) without any explicit agreement between firms. Independently designed algorithms, each optimizing for its own profit, might learn to avoid price wars and coordinate tacitly to keep prices high. This is essentially the classic oligopoly tendency (a few firms gravitating toward stable high prices) accelerated by AI.

Evidence from Theory: Research shows that self-learning algorithms can reach supra-competitive pricing strategies on their own. For example, Calvano et al. (2020) experimented with Q-learning AI agents in a repeated pricing game; the algorithms consistently learned to charge supracompetitive prices without communicating. The AI agents effectively discovered a cartel-like strategy: keep prices high most of the time, punish any rival's price cut with a brief price slash (a "price war" punishment), then return to high prices. This pattern emerged even though each algorithm was simply told to maximize its own profit, not to collude. Similarly, other simulations using multi-armed bandit algorithms found that independent pricing agents can gradually synchronize on high prices by observing and responding to each other's pricing patterns, essentially "learning" that aggressive competition is not rewarded. These studies highlight how algorithms may form stable high-price equilibria that are hard to distinguish from conscious collusion. In one joint agency report, enforcers noted that algorithms can "calculate a high price that reacts to changing market conditions and benefits all competitors; the speed at which they detect and respond to deviations reduces the incentive to undercut, so prices remain above competitive levels even without explicit collusion." In other words, algorithms can undermine competitors' incentives to cut prices, since any price drop by one is immediately matched by others, keeping the overall price level high. This creates both false positives (authorities might suspect collusion where it's just autonomous algorithmic adaptation) and false negatives (truly collusive outcomes that escape punishment because no formal agreement exists). It is important to emphasize that algorithmic performance may lead to the stabilization of prices at supra-competitive levels, even in the absence of explicit coordination among firms. Certain features inherent to artificial intelligence algorithms contribute to this outcome, particularly their increasing tendency to prioritize exploitation over exploration in decision-making processes. This dynamic may result in independent yet convergent pricing strategies among competing firms, each focused on maximizing its individual margins. Consequently, this scenario produces a de facto alignment of market conduct that closely resembles the effects of collusion, despite the absence of overt agreements or direct communication among market actors (Abada et al., 2024).

Hub-and-Spoke via Common Algorithms: Another scenario is collusion through a shared algorithmic platform. If competing firms all rely on the same third-party pricing software or data platform, it can act as a central "hub" that aligns their pricing. The shared algorithm, using data from all clients, could effectively optimize joint profits as a cartel would. A real-world example is the ongoing RealPage (YieldStar) case in the U.S., where numerous landlords used a common rent-pricing software that analyzed industry data and allegedly led to coordinated rent increases across properties (see for a synthesis Marty, 2025). Lawsuits and government investigations allege that RealPage's algorithm, armed with private data from competing landlords, effectively recommended synchronized price hikes, pushing rents up by 5% or more beyond market rates. In essence, the platform may have served as a collusive hub, telling each landlord not to undercut the others. Likewise, in the EU's Eturas case (2016), dozens of travel agencies used the same online booking system, whose operator imposed a uniform cap of 3% on discounts. The European Court of Justice held that if the agencies were aware of this algorithm-imposed restriction (they were notified via the system) and did not object, they could be found part of a concerted practice. In other words, firms cannot escape liability by "hiding behind" a common algorithm – merely using a shared pricing tool that restricts or aligns prices can be enough to infer an agreement, especially once firms know about the practice and acquiesce.

Competing firms may actively contribute to the emergence and stabilization of supra-competitive pricing equilibria by engaging in a variety of facilitating practices. Firstly, firms may reinforce supra-competitive pricing patterns through algorithmic signalling. Secondly, a similar outcome may be achieved by designing algorithms in ways that maintain sufficient interpretability by competitors—thus generating artificial transparency. This scenario differs from the previously described one insofar as these deliberate actions (or deliberate omissions, in the second case) may constitute 'plus factors' intended to sustain a collusive equilibrium (see Marty & Warin, 2024, for a detailed discussion).

To address such collusive or pseudo-collusive risks, ex ante regulatory measures may be implemented, requiring firms to adopt compliance procedures that ensure an appropriate level of precaution against collusive or quasi-collusive outcomes—specifically, the emergence of supra-competitive prices. Additionally, firms found to be non-compliant or negligent may be held liable under existing legal frameworks (see de Marcellis-Warin et al., 2025, for an overview).

"Oligopoly 2.0" – Autonomous Collusion: The broader worry is that algorithmic pricing could **make tacit collusion more pervasive and stable** – effectively an "oligopoly problem 2.0." Markets that were previously competitive might converge to high-price equilibria as algorithms relentlessly optimize and retaliate. Because algorithms react instantaneously to each other, any attempt by one firm to cut price and gain market share can be immediately met by matching cuts from others, rendering the price cut futile. Knowing this, each algorithm learns that keeping prices high yields better long-run profits for all, and that deviating (competing on price) only triggers a price war with no lasting gain. Over time, the industry settles into a silent coordination at elevated prices. Crucially, current laws struggle to address this. Tacit collusion (parallel pricing without an agreement) is not illegal under most competition laws – enforcement typically requires evidence of a communication or "meeting of minds." If algorithms independently achieve a collusive outcome, it may fall entirely outside the reach of antitrust law, despite consumers paying more. This enforcement gap has fueled calls for new approaches. Early empirical evidence adds urgency: for instance, a recent study of gas stations in Germany found that stations using an AI pricing algorithm saw profit margins increase by around 5%, and as more stations adopted the same tool, prices in local markets stabilized at higher levels (Assad et al., 2024). Similarly, research on U.S. e-commerce showed that retailers employing pricing algorithms tended to charge higher prices than those not using algorithms, all else equal. These findings suggest algorithm-driven supra-competitive pricing is already occurring without explicit collusion.

Policy Implications: Tackling algorithmic tacit collusion is challenging, as it may require moving beyond the traditional insistence on proof of agreement. Experts have proposed creative solutions. One idea is to shift the burden of proof or create outcome-based liability in suspect scenarios. For example, if an industry with only a few players and heavy algorithm use exhibits sustained parallel high prices unexplained by costs, authorities could presume anti-competitive coordination and require the firms to demonstrate that their algorithms operate independently and pro-competitively. Another proposal is mandated algorithmic transparency or audits. Companies might be required to hand over their pricing algorithms (or at least detailed logs of algorithmic decisions) to competition authorities for review. This could help detect whether an algorithm is effectively "coding" tacit collusion (e.g. always matching rivals' prices within seconds or using punish-then-reward patterns). However, because sophisticated machine learning algorithms can learn collusive strategies without being explicitly programmed for them, simply reviewing code may not reveal anti-competitive behavior. Regulators may need to test algorithms in controlled simulations or use their own AI tools to probe how industry algorithms respond to various scenarios. Some jurisdictions are considering ex ante rules. The UK's proposed Digital Markets Unit (DMU), for instance, could get powers to set conduct standards for dominant firms' algorithms, potentially including pricing algorithms. Ideas floated include requiring a degree of randomness in pricing algorithms (to prevent perfectly in-sync price moves) or prohibiting algorithms that respond too instantly and uniformly to competitors. A blunter approach would be to bar competitors from using the same pricing service to avoid hub-and-spoke collusion: if many firms need algorithmic pricing, ensure they each use different providers or siloed systems so no single hub has all the data[4].

Additionally, competition agencies might treat the sharing of real-time pricing data among competitors as inherently risky – much as they treat exchange of future price plans as presumptively collusive. Any intervention, however, must balance the risk of chilling beneficial uses of algorithms. Overly strict rules could discourage companies from adopting pricing innovations that genuinely lower costs or benefit consumers. Thus, many suggest a calibrated approach: closely monitor markets most prone to algorithmic collusion (concentrated, transparent-price industries) and be ready with updated tools (like algorithm audits or interim measures) when suspicious patterns appear. International cooperation will also be important, since algorithms deployed by global firms could collude across borders – competition authorities are increasingly sharing techniques to detect and address algorithmic collusion scenarios[5].

4. Dynamic vs. Personalized vs. Manipulative Pricing

Not all algorithmic pricing is alike. It's important to distinguish legitimate dynamic pricing, personalized price discrimination, and manipulative pricing tactics, as each has different implications for consumers and competition (see Marty et Warin, 2023b for a synthesis on algorithmic-based unilateral anticompetitive risks):

---

[4] These issues also carry significant implications for another branch of competition law: merger control. They highlight the importance of close scrutiny where a transaction reduces competition in sensitive sectors such as pricing and revenue management tools—particularly in terms of the number of independent players and the enhanced data-related competitive advantage of the merged entity. Two challenges must be considered in this context.
First, it may be necessary in some cases to intervene below traditional structural thresholds, especially where the target firm does not hold a substantial market share but possesses data assets of strategic value. However, any broadening of the scope of ex ante merger control raises the risk of over-enforcement, with competition authorities potentially burdened by an influx of transactions to assess—many of which may pose only limited competitive risks. Intensified scrutiny must therefore be evaluated through a cost-benefit lens, taking into account the administrative capacity of the authority and the potential competitive harm. Second, where merger control is deployed to address such risks, it becomes essential to design effective behavioural remedies. Prohibition of a transaction may entail significant opportunity costs in terms of foregone efficiency gains. In cases where the merger may result in a form of tacit coordination through a shared algorithmic infrastructure or common developer, specific behavioural commitments could be envisaged—such as the adoption of decentralised learning architectures or the introduction of randomisation mechanisms in pricing recommendations.

[5] Such dimensions underscore the interest of market supervisory authorities in developing algorithmic oversight tools, in line with initiatives falling within the scope of computational antitrust (see Nazzini and Henderson (2024) for a recent application).

- **Dynamic Pricing (Surge/Yield Pricing):** Dynamic algorithms adjust prices rapidly in response to real-time market conditions – for example, increasing prices when demand surges or supply is limited, and decreasing prices when demand softens. This practice is largely driven by efficiency. By raising prices during peak demand (and lowering them in off-peak times), dynamic pricing allocates goods and services to those who value them most at that moment and can prevent shortages or congestion. Classic examples include ride-hailing apps using surge pricing during busy hours, airlines and hotels changing fares based on booking demand, or electricity providers charging higher rates at peak usage times. Properly implemented, dynamic pricing increases total welfare: it signals consumers to adjust their consumption (e.g. travel at off-peak times to save money) and incentivizes suppliers to expand capacity when it's most needed. It can also spur short-run competition – if one firm's algorithm aggressively discounts excess inventory or unpopular time slots, rivals may have to match those lower prices to avoid losing business. As a result, dynamic pricing per se is not viewed as problematic under competition law. Regulators typically only step in to ensure transparency (so consumers understand price fluctuations) or to curb extreme cases of price gouging (many jurisdictions have laws against exploitative price hikes during emergencies). Overall, dynamically adjusting prices in line with supply and demand is seen as a legitimate, often beneficial use of algorithms.
- **Personalized Pricing (Price Discrimination):** Personalized pricing means offering different prices to different customers based on data about each customer's characteristics or behavior. Algorithms facilitate this by analyzing factors like a user's purchase history, location, browsing habits, or device, to estimate their willingness-to-pay. The welfare impact of personalized pricing is mixed and context-dependent. Some consumers – especially price-sensitive ones – may benefit. For example, an algorithm might detect that a certain customer only buys when prices drop and offer them a special discount, or a new platform might show lower prices to first-time users to encourage trial. In competitive markets, such personalization can intensify competition: firms will strive to give the best deal to win each customer from rivals. Indeed, personalized promotions can help challengers poach loyal customers from big firms, which is pro-competitive in effect. However, in less competitive settings (e.g. a dominant platform or a market with few alternatives), personalized pricing often means loyal or captive customers pay more, while only the most fickle, likely-to-switch customers get deals. This "loyalty penalty" is well-documented in markets like telecoms, insurance, and subscriptions: long-time customers face steadily rising prices, whereas

new subscribers or those who threaten to leave receive retention offers[6]. Algorithms greatly enhance firms' ability to execute such strategies, by continually identifying who is less likely to churn and charging them higher margins. From a legal standpoint, price discrimination on its own is usually not illegal (except when it involves selling below cost in a way that harms competition, or when it implicates protected classes of consumers which falls under anti-discrimination laws). But competition authorities scrutinize it if a dominant firm uses personalization to exclude competitors or exploit consumers. For instance, if a dominant online platform routinely shows higher prices to users who almost never comparison-shop, that could be viewed as exploiting its market power over that segment. There's also a broader fairness and transparency issue: consumers often feel it's unfair to charge different people different prices for the same product. The opacity of algorithms makes it worse – people may not even know they're paying a personalized premium. In response, policymakers have started pushing for transparency. New York State enacted a law in 2025 requiring that online businesses clearly notify consumers when a price is set by an algorithm using their personal data. The goal is to alert consumers that an offer might be personalized, prompting them to shop around or opt out. Competition agencies, alongside consumer protection bodies, are considering whether undisclosed personalized pricing might qualify as a deceptive practice in some cases. At minimum, they are keeping an eye on whether personalization leads to outcomes like certain demographics or vulnerable groups systematically paying more (which could also raise equity concerns or violate other laws).

- **Manipulative Pricing (Dark Patterns and Exploitation of Biases):** A more insidious category is manipulative or deceptive or even manipulative pricing and commercial practices, where algorithms set prices or present offers in a way designed to *exploit cognitive biases or information asymmetries* in consumers. This goes beyond simply charging what the market will bear; it involves tricking or pressuring consumers into suboptimal choices (de Marcellis-Warin et al., 2022). Examples include using dark patterns in online interfaces: an algorithm might display a false scarcity message ("Only 2 left at this price!") or a countdown timer to create a false sense of

[6] Consumers using a competing service are likely to be targeted with more advantageous offers than those made available to individuals who have already subscribed, reflecting a strategy of data-driven discrimination and customer lock-in. Much like within digital ecosystems, complementors pursuing a single-homing strategy may progressively face a deterioration in the terms and conditions governing their access, reflecting the increasing asymmetry in bargaining power vis-à-vis the platform (see Marty and Warin, 2023c).

urgency, inducing the user to buy immediately at a higher price than they might otherwise pay. Another tactic is price steering or personalized framing – for instance, an algorithm detects that a customer has viewed a product multiple times without purchasing and then raises the price slightly on the next visit while suggesting "prices may rise soon," exploiting the fear of missing out to push the consumer into buying. Some e-commerce algorithms also use tricks like hiding cheaper options or add-on fees until late in the checkout process (so-called drip pricing). These strategies can maximize the seller's revenue but leave consumers worse off – they may end up paying more for the same product or buying extras they don't need due to deceptive influence. Unlike transparent price discrimination (where a consumer at least knowingly pays a certain price), manipulative pricing *undermines genuine consumer choice*. It borders on or crosses into fraud and false advertising. Regulators typically address such practices through consumer protection laws. For example, the US Federal Trade Commission, the UK Consumer and Markets Authority (CMA), and the Australian Competition & Consumer Commission have all taken action against various online dark patterns, such as undisclosed fees and fake countdown timers, under laws against unfair or deceptive acts. The competition law angle comes into play if a dominant firm is using manipulative design to maintain or extend its market power – for instance, if a dominant online marketplace designs its algorithm and interface to down-rank competitors' products or to keep users from finding external offers (thus excluding rivals through deception). In such cases, a manipulative pricing scheme could be treated as an exclusionary abuse of dominance in addition to a consumer protection violation. Detecting manipulative pricing is challenging because these tactics are often personalized and continuously A/B tested. The "evidence" of the practice (like a fake urgency prompt) might only appear for certain users under certain conditions, making it hard for outsiders to systematically observe. To tackle this, authorities are beefing up their tech tools – for example, deploying web-scraping bots or even their own machine learning systems to act as "mystery shoppers" online and detect patterns of deceit. Some experts have suggested empowering consumers with countermeasures: for instance, browser extensions that alert users if a price they're seeing is higher than what other users were offered, or that flag when a website is using known dark patterns. Additionally, there are calls for companies to implement internal algorithmic compliance programs – basically, to regularly audit their own pricing algorithms for manipulative or biased outcomes, much as they audit for data privacy compliance. Competition agencies may encourage such self-regulation as a supplement to enforcement, especially since catching every dark pattern in real time is difficult. The overarching principle is that algorithmic pricing must not be allowed to undermine consumer autonomy or hide the true price. Whether through competition law (if it impacts market fairness) or consumer protection law (if it's deceptive), regulators are intent on curbing manipulative algorithmic practices.

5. Data and Algorithm Design: Competitive Concerns

Pricing algorithms run on data; thus, data collection, sharing, and algorithm design choices can themselves raise competition issues:

- **Internal Data and the "Loyalty Penalty":** A firm's first-party data – detailed information on its own customers' purchasing habits, browsing, and responsiveness to prices – is a double-edged sword. It can improve efficiency (enabling more tailored offers) but also enable the firm to exploit its loyal customer base. Ironically, the customers who are most loyal (and thus provide the most data) are often targeted at higher prices. An algorithm armed with extensive data on a customer can predict they are unlikely to switch to a competitor, and accordingly it may steadily raise that customer's price to increase margins. Meanwhile, for a new customer or one who sporadically shops around (providing less data and showing less loyalty), the firm's algorithm might offer a *discount* or promotion to win their business. In effect, loyalty is punished with high prices, while disloyalty is rewarded with bargains. This dynamic – the loyalty penalty – is a sign of market power over locked-in consumers. If customers were freely able to switch and aware of alternatives, the firm couldn't get away with charging loyal users more. To combat this, policy measures focus on reducing switching costs and giving consumers control of their data. For instance, regulators and consumer advocates encourage the use of price comparison tools and easy cancellation processes, so that even long-time customers can easily check if they're getting a bad deal and change providers. Data protection laws (like the EU's GDPR) also help by allowing consumers to limit tracking or port their data to other services. Data portability means a customer can take the record of their purchases and preferences from one platform and share it with a competitor to obtain a better offer. If widely implemented, this can undermine a dominant firm's data advantage – rivals can compete for even the loyal customers by leveraging the same data (with permission). Some jurisdictions also consider **"fair by design"** principles – urging that algorithms should not systematically treat long-term customers worse than new ones, or at least that firms should periodically inform loyal customers about available discounts. While not strictly antitrust, these consumer empowerment steps have competitive implications: they make it harder for a company to hide behind data asymmetry and milk a locked-in user base.

- **Third-Party Data and Analytics:** Beyond internal data, companies often purchase data or subscribe to analytics services that aggregate industry information. For example, firms might use a service that tracks competitors' prices in real time, or that provides market-wide sales trends. While these can be legitimate tools, widespread reliance on the *same* data sources can lead to indirect information sharing and coordination. If all major competitors see the same dashboard saying "market demand is up 10% and average industry price is $X," it's easier for all of them to raise their prices in unison. Essentially, sharing detailed market data can synchronize firms' behavior. Competition law has long been wary of competitors exchanging sensitive information (like future pricing plans or granular sales data) because it can facilitate tacit collusion. In the algorithmic era, information exchanges may happen through data brokers or cloud analytics platforms rather than an old-fashioned cartel meeting. The onus may fall on regulators to ensure that industry data platforms do not enable collusion. This could mean encouraging only aggregated or delayed data sharing (so firms can't react instantly to each individual rival's moves) or monitoring whether companies that use the same analytics show suspiciously aligned pricing. If an analysis finds that firms all respond to market changes in lockstep due to a common data input, authorities might treat that as a facilitating practice. In some cases, competition agencies might even advise against an entire industry relying on a single data provider, or impose **firewalls** preventing a data service from telling each client exactly what the others are doing. The goal is to preserve some uncertainty and independence in firms' decision-making.

- **Common Algorithm Developers and Data Pooling:** As noted earlier, when competitors outsource their pricing optimization to the same algorithm or AI developer, it raises a red flag. If, say, five retailers all hire the same AI company to manage pricing, there's a risk that the AI's model is effectively trained on pooled data from all five and figures out a strategy that maximizes the group's profit rather than fostering competition. This could happen even if the AI company doesn't intend it – a sophisticated algorithm might discover that coordinating pricing yields higher rewards and implement that pattern across all its clients. From a liability perspective, competition law may treat this as a hub-and-spoke conspiracy or at least a concerted practice facilitated by a common agent. A firm can't simply say "my vendor set the price, not me." If the outcome is anti-competitive, both the firms and the vendor could be held responsible. To mitigate this, companies using third-party pricing algorithms may need to exercise a duty of vigilance: they must ensure (via contract or due diligence) that the provider will not use their data to help competitors or will not create a unified model across rivals. Competition authorities might issue guidance or even requirements that pricing AI providers separate data and models for each client unless clients are part of the same corporate group. In some situations, authorities could go as far as prohibiting direct competitors from using the same pricing platform if it effectively means sharing a brain. If anti-competitive outcomes are detected, remedies might include requiring the common provider to modify how its algorithm works or to stop serving multiple rivals in that market. A notable historical analogy is the Airline Tariff Publishing Company (ATPCO) case in the 1990s, where U.S. airlines were indirectly coordinating fares by posting fare changes with future effective dates on a shared platform. Enforcers intervened to stop that signaling (Marty et Warin, 2024). Today's analog might be intervening if, for example, a cloud AI service is found to be coordinating prices among client firms. Ultimately, the principle is that outsourcing to an algorithm doesn't shield companies from antitrust law: if you delegate pricing to a third party, you are accountable for the results just as if you'd made the decisions internally.

- **Algorithm Design and Learning Parameters:** The design choices in algorithms can themselves impact competition. For instance, a centrally trained AI model (one that learns from multiple sources or markets together) might internalize strategies that reduce competition (like avoiding price undercutting) more readily than separate models trained in isolation would. Regulators may actually prefer a landscape of diverse, independent algorithms making decisions, rather than one "super-algorithm" optimizing an entire market. Additionally, certain types of algorithms may inherently collude or exclude. Reinforcement learning algorithms, depending on how they are rewarded and if they factor in rivals' actions, might consistently find cooperative (collusive) equilibria. If research and experiments show that a particular algorithmic strategy (say, a strategy that instantly matches any competitor price drop) leads to higher prices for consumers, there could be pressure to discourage that strategy. While competition agencies typically don't dictate how companies design software, they are exploring ways to audit algorithms and possibly issue guidance. The UK's CMA, for example, has a data unit examining how algorithms across online platforms affect outcomes for consumers. In one scenario, a regulator could discover that a company's pricing algorithm was effectively using competitors' prices as an input and always raising its own prices to just follow the highest competitor. The regulator could then demand that the company adjust the algorithm to introduce more independent pricing or face action for tacit coordination. In extreme cases, one could imagine regulators saying that certain algorithmic features (like real-time competitors price matching) are presumptively anti-competitive for a dominant firm. Any such measures would be controversial, but they underscore the growing view that firms are responsible for how their algorithms behave, and that means the data and design feeding those algorithms are fair game for competition scrutiny.

So, **controlling data flows and algorithm usage is key to maintaining competition** in algorithm-driven markets. Measures that promote data mobility (so consumers and smaller rivals can access data that big firms hold) and that prevent excessive data concentration help level the playing field. Privacy laws limiting data collection can incidentally prevent the most extreme personalized pricing. Conversely, transparency in data sharing arrangements can expose if firms are effectively colluding via shared analytics. By ensuring that no single platform or algorithm has an unbeatable data advantage, authorities aim to keep markets contestable. This leads into the next topic: how dominant platform ecosystems can use algorithms and data to lock in users and partners.

5.1 Ecosystem Lock-In and Single-Homing

In digital markets, powerful platform ecosystems (such as dominant e-commerce marketplaces, app stores, or ride-hailing platforms) can leverage algorithmic pricing to reinforce lock-in for both consumers and business partners. A key concept is the contrast between single-homing (using one platform exclusively) versus multi-homing (using multiple competing platforms). Dominant firms frequently attempt to induce market participants to adopt single-homing practices, thereby reducing competition and increasing their capacity to extract surplus. Bougette et al. (2022) provide an analysis of self-preferencing strategies, characterizing these practices as not merely exclusionary abuses but also exploitative ones.

Algorithms Encouraging Single-Homing: Dominant platforms can use pricing algorithms as both carrot and stick to keep users and partners from straying. For consumers, a platform might deploy personalized discounts or loyalty rewards to entice them to stick around, and especially to win back those who try a competitor. For example, if a user starts using a rival ride-hailing app, the dominant app’s algorithm might detect this (perhaps via decreased usage or even device data) and respond by offering that user special coupons or lower prices for a while to win them back. This is a pro-competitive incentive in the short term (the user gets a deal), but it’s selectively applied only when competition looms. Meanwhile, consumers who have shown no interest in alternatives – the truly loyal ones – may quietly see prices creep up (the earlier-mentioned loyalty penalty). Thus, the platform maximizes revenue from its locked-in base and only sacrifices margin when a user's behavior suggests they might switch (Marty et Warin, 2023c). For business partners (like third-party sellers on a marketplace, or drivers on a ride-sharing platform), algorithms can implicitly enforce exclusivity. A platform can program its search ranking or "buy box" algorithm to favor those partners who stay exclusive or at least don't undercut the platform's prices elsewhere. For instance an E.U. Commission commitments decision states that Amazon's algorithms may have historically given the coveted "Buy Box" (the default purchase option) to sellers who offer the lowest price on Amazon. If a seller lists a product cheaper on a rival site, Amazon's algorithm can detect that and may suppress that seller's listing or lose them the Buy Box on Amazon, leading to a sharp drop in sales for that seller. This creates a powerful incentive for sellers to price uniformly or higher on other platforms, effectively an algorithmic MFN (most-favored-nation clause): the platform ensures no one else offers a better deal (see Mouton and Rottembourg, 2024, for an in-depth analysis of the behavioral commitments resulting from this decision). Similarly, a dominant food delivery app might use an algorithm to deactivate or penalize restaurants that give better prices on a competing app. The restaurant might not be explicitly forbidden from multi-homing, but in practice they learn that doing so hurts their visibility or volume on the dominant app. Over time, both users and partners gravitate toward single-homing on the dominant platform because that's where they get the best personalized deals or exposure.

Exclusivity and Retaliation: Traditional competition enforcement has dealt with explicit exclusivity contracts and MFN clauses as potentially anti-competitive. Many of those (like broad retail MFNs used by online travel agencies or most-favored-pricing clauses used by Amazon in the past) have been challenged or voluntarily dropped under regulatory pressure. However, algorithmic enforcement is more subtle. There may be no written rule saying "don't list elsewhere for less," but the platform's automated systems create a de facto rule. This can actually be harder to detect and prove: each individual seller or user just experiences a tailored consequence (a lost promotion here, a higher price there), and there's no single policy document to point to. Nonetheless, competition authorities are becoming attuned to patterns that suggest systematic retaliation. If, for example, numerous businesses report that the only variable explaining a drop in their sales on a platform was that they started offering lower prices on another site, that's circumstantial evidence the platform's algorithm is enforcing an anti-competitive norm. Such behavior, if by a dominant firm, could be viewed as exclusionary – similar in spirit to an exclusive dealing arrangement or predatory strategy. The difference is it's personalized and hidden in the algorithm's black box.

Consumers Trapped in Ecosystems: From the consumer perspective, algorithmic lock-in can lead to monogamy with the platform even absent formal lock-in. Users might initially enjoy perks – e.g. a streaming service bundles free shipping and discounts (Amazon Prime model), or a ride app gives loyalty points for frequent riders. These benefits, optimized by algorithms, make the overall ecosystem more convenient and cost-effective than piecing together services from multiple providers. If a user occasionally tries a competitor that offers a cheaper price on some item, the dominant platform's algorithm might match that price just for that user ("price matching" on an individual level) to prevent defection. The user thus comes to believe the dominant platform will always be competitive for them and stops checking alternatives – a phenomenon sometimes called "learned loyalty". The immediate outcome is that the user is getting good deals due to competition for their attention. But the long-term outcome is reduced competition: the rival platform never gains enough users to pose a serious threat because every time it offers an enticing deal, the dominant platform algorithmically neutralizes the threat for those users. Eventually the rival may give up or stagnate. At that point, the dominant platform no longer needs to offer special inducements; it can even start raising prices or fees for everyone, including previously wooed users, because the competitive pressure has diminished. This is how markets tip to a winner-take-all outcome. Data plays a crucial role here as well: the longer a user stays on one platform, the more data the platform has to serve them well (through personalization and convenience), which competing services can't easily replicate. This data network effect means the dominant firm's service genuinely becomes better for that user, independent of network size, creating a feedback loop where the more you use it, the harder it feels to leave.

Long-Term Dependency Harms: When single-homing becomes the norm, market contestability suffers. A small business that relies on a dominant marketplace for, say, 80% of its sales is effectively at that platform's mercy. If the platform raises commission fees or changes its algorithm in a way that disadvantages that business, the business has little recourse – it has lost direct contact with customers and alternative channels are weak. Similarly, consumers who rely on one super-app for all their needs might face a lack of real choice if that app starts tightening terms or exploiting its position. These situations can lead to higher prices, reduced innovation (as rivals can't get a foothold to challenge the incumbent), and a general shift of bargaining power in favor of the dominant firm. In competition terms, this is an entrenchment of dominance through technical means rather than explicit agreements.

Potential Remedies: Preserving competition in the face of algorithmic lock-in requires reducing switching frictions and opening up ecosystems:

- **Ban Explicit Exclusivity Practices:** As a baseline, authorities can prohibit formal agreements that reinforce single-homing. Many jurisdictions already scrutinize or ban wide price parity clauses (which prevent sellers from offering lower prices elsewhere) and certain loyalty rebates that lock in customers. Ensuring these rules cover algorithm-driven equivalents is important. If evidence shows that a platform's algorithm punishes off-platform discounts, the platform could be warned or penalized just as if it had an illegal MFN clause. For example, competition agencies could treat an algorithmic retaliation scheme as an abuse of dominance, ordering the platform to cease such conduct. This might involve mandating transparency – e.g., requiring a dominant marketplace to inform sellers how its ranking algorithm works with respect to external prices, which pressures the platform to keep it neutral.
- **Data Portability and Interoperability:** A powerful tool to counter lock-in is giving users control of their data and requiring dominant platforms to be interoperable to some degree. **Data portability** means a consumer or business can easily take the data they've generated on one platform and transfer it to another. For instance, a merchant could export their product reviews and sales history from Amazon and import them to a new marketplace, so they don't have to start from zero. Likewise, a social media user could move their content and contacts elsewhere. When users know they won't lose everything by switching, they are more willing to try alternatives, which in turn forces the dominant firm to compete on merit rather than complacently relying on captive users. Interoperability goes further – it can require the dominant platform to allow interactions with other services. For example, WhatsApp was pressured to allow users to port chats or communicate with other messaging apps in some jurisdictions. In commerce, one could imagine rules that a dominant app store must permit price comparison tools or that a dominant ride-share must allow drivers to use multi-homing software.
- **Monitoring and Early Action:** Competition authorities should monitor markets for selective discounting patterns that indicate predatory targeting of entrants (which is discussed more in the next section). If a dominant firm is only offering big discounts in a region or segment where a new competitor operates (while keeping prices high elsewhere), agencies can intervene sooner rather than later. Traditional predatory pricing cases require proving intent and likelihood of recoupment, which can be slow; but given the speed of algorithmic strategies, regulators might use interim measures (temporary orders) to stop such practices while investigating. Similarly, if a dominant

platform suddenly increases fees for partners right after a rival exits the market, that could confirm anti-competitive lock-in. Keeping a close eye on such metrics – and perhaps requiring dominant firms to report certain pricing moves or algorithm changes in core markets – can help catch anti-competitive lock-in strategies in the act.

- **Ex Ante Regulation for Gatekeepers:** As mentioned, regulations like the EU DMA or proposals for digital platform oversight in other countries include provisions to address lock-in. These might mandate, for example, that platforms cannot prevent businesses from communicating with customers acquired on the platform (so a seller could email a customer and offer them to buy direct next time, something platforms often restrict). They may also require algorithmic transparency and fairness – for instance, requiring that ranking algorithms are not biased against offers that are available cheaper off-platform. If a platform knows it must treat outside offers fairly in its algorithm, it will be less able to enforce de facto exclusivity. Such regulations are proactive and broad-brush, but they provide clear rules of the road that limit how far a dominant firm's algorithms can go in squeezing out competition.

These considerations invite broader reflection on the complementarity and interactions between competition law and regulatory frameworks within the digital sphere (Bougette et al., 2025). As with any form of ex ante intervention, regulation holds a legitimate role when it prevents irreversible harm or facilitates effective ex post enforcement of competition rules—as exemplified notably within financial markets. Nevertheless, in sectors characterized by rapid technological evolution and competitive volatility, regulatory interventions should adopt a light-touch approach to avoid excessive costs and potential efficiency losses. Consistent with recommendations advanced by Tirole (2023), regulatory oversight should ideally be entrusted to the competition authority itself, thereby minimizing overlaps or jurisdictional conflicts among regulators responsible respectively for safeguarding competition, protecting consumers, or overseeing trading relationships.

Within this logic, regulatory actions should prioritize promoting data portability, ensuring service interoperability, and restricting contractual provisions that incentivize single-homing, among other objectives. The overarching aim of these interventions is to preserve market contestability and ensure fairness within competitive dynamics. Although these objectives resonate closely with the rationale underpinning the European Union's Digital Markets Act (DMA), the mechanisms deployed to achieve them may be more diverse and flexible—ranging from co-regulatory frameworks to intervention models informed by industry codes of conduct.

A critical challenge concerns the practical implementation of flexible or adaptive regulatory rules, particularly those entailing behavioural obligations. In volatile markets marked by swift technological developments, adaptability is crucial. Such flexible oversight is pertinent both to remedies imposed in antitrust cases (such as injunctions or commitments) and to corrective measures within merger control proceedings (Bougette et al., 2024).

5.2 Algorithmic Unilateral Strategies: Predation and Segmentation

Algorithms not only collude; they can also sharpen unilateral anti-competitive strategies by dominant firms, such as predatory pricing (see Cheng and Nowag, 2023, for instance) or foreclosure schemes, making them harder to detect:

Granular Predatory Pricing: Traditional predatory pricing involves a dominant firm pricing below cost widely to drive out a competitor, then raising prices later to recoup losses. It's risky and rarely observed because it harms the predator in the short run and is hard to pull off. Algorithmic pricing, however, enables a form of selective predation that is subtler. A dominant platform can algorithmically target only the customers or regions where a new competitor is trying to gain a foothold and offer those customers extremely low prices (even below cost), while maintaining higher prices for everyone else. Because this targeted strategy is cross-subsidized by the profits from the non-contested customers, the dominant firm might never incur an overall loss – in fact it might remain profitable even during the "predatory" campaign, obscuring the strategy from standard financial analysis. For example, imagine a dominant grocery delivery service that faces a new rival in one city. The incumbent's algorithm could identify all users in that city (or even specific zip codes) who have tried the rival app and then offer those users huge discounts or free deliveries to retain them. At the same time, users in cities with no rival continue paying normal (higher) prices. The revenue from the untouched markets covers the aggressive discounts in the contested city. The rival struggles because every time it attracts a customer with a lower price, the dominant firm swoops in and undercuts that price for that customer via personalized offer. Over time, the rival cannot build a customer base and exits. The dominant firm has predated – but not in the classical way of bleeding money market-wide. Antitrust enforcers looking at aggregate data might see that the firm never priced below cost on average, or that its overall margins stayed healthy, and thus might miss the predation. To catch this, authorities need to look at granular data: prices and costs by customer segment or locality. If they find a pattern like "Firm A offered a 50% discount to all customers of Competitor B, while charging full price to others," that's strong evidence of a targeted exclusionary strategy.

Personalized Exclusion (Loyalty Schemes 2.0): Another unilateral tactic is using algorithms to implement what are effectively exclusive dealing or loyalty rebate schemes, but personalized. In the past, a dominant firm might say to a customer or supplier: "Take 100% of your business with me, and you get a 10% rebate on everything." That could be illegal if it locks the customer away from rivals. Now, an algorithm can do this quietly: it can observe a buyer's split of purchases and, if it sees them shifting some share to a rival, automatically increase the discount or offer a special deal to entice them back to full loyalty.

Market Segmentation and Implicit Division: Perhaps the most intriguing algorithmic strategy is where competing firms implicitly divvy up the market through their independent algorithms' decisions. Consider two major firms in a market. Over time, Firm A's algorithm might learn that it makes the most profit by focusing on high-end consumers with high prices, and every time it tried to cut prices to grab price-sensitive consumers, Firm B matched and profits fell. Meanwhile, Firm B's algorithm learns it maximizes profit by catering to price-sensitive consumers with lower prices, and if it tries to raise prices, Firm A undercuts and it loses share. So A sticks to the premium segment, B sticks to the budget segment, and they avoid encroaching on each other. There's no agreement or even communication – just years of reactive pricing that taught each algorithm its "turf." The result is a stable duopoly where each firm has market power over "its" segment: firm A's wealthy customers face A's monopoly-like high prices (because B isn't trying to serve them), and firm B's frugal customers face B's constrained choices (because A isn't offering them something better). Essentially, the market gets partitioned. This is akin to market allocation which is per se illegal if done by agreement – but here it's achieved tacitly via algorithms optimizing in parallel. Traditional antitrust again finds this hard to tackle because there's no communication to ban. Yet consumers are clearly harmed by the lack of cross-segment competition. One approach to addressing this could be through oligopoly regulation or oversight (outside the current antitrust framework), where authorities might intervene if they see that segments of consumers are not benefiting from competition due to stable patterns of non-interference between leading firms.

Enforcement Approaches: To handle these unilateral algorithmic strategies, competition agencies may need to both sharpen existing tools and invent new ones:

- **Refined Predatory Pricing Tests:** Authorities could update their guidelines to clarify that **selective below-cost pricing** aimed at eliminating a competitor is just as illegal as across-the-board predation. This means looking beyond firm-wide profitability and assessing the intent and effect on a targeted basis. If a dominant firm's algorithm is giving deals that make no business sense except to prevent switching to a rival, that could satisfy the "no economic sense" or "sacrifice" test for predation.

- **Interim Measures and Quick Reaction:** Given the speed at which an algorithm can drive a rival out, agencies should be prepared to act quickly. This could involve seeking preliminary injunctions in court or imposing interim orders administratively to stop a dominant firm from continuing a suspicious pricing campaign.

- **Collaboration with Sector Regulators:** Many industries with dominant players have specialized regulators (telecom, energy, banking) who monitor pricing and market behavior in detail. These regulators might spot algorithmic abuses early. For instance, a telecom regulator might notice an incumbent offering generous "win-back" discounts to customers who try to switch providers, which could be an exclusionary strategy. By working together with the competition bureau, they can address the issue from both regulatory and antitrust angles. In some cases, a sector-specific regulator (or the competition authority itself) could directly sanction the behavior under consumer fairness rules, or refer evidence to the competition authority for antitrust action. This kind of cross-agency teamwork will be increasingly important as pricing strategies blend competitive and consumer protection issues.

Co-regulatory and compliance-based approaches may prove particularly effective when addressing potential algorithm-driven anticompetitive practices, whether these involve coordinated conduct (such as collusion or parallel behaviour) or unilateral strategies (including self-preferencing, price discrimination, exclusionary pricing, or consumer manipulation). In this context, algorithmic oversight should be exercised through both ex ante and ex post interventions.

Ex ante, procedural safeguards or certification standards for algorithms—a form of algorithmic due diligence—could be envisaged, alongside collaborative experimentation between firms and competition authorities facilitated through regulatory sandboxes. Ex post, algorithmic systems should be subject to direct internal oversight at the point of implementation; the deploying firm is, in principle, best positioned to identify potential harms at an early stage and mitigate them at the lowest possible cost.

Additionally, firms may be subject to data or code disclosure obligations, which in turn could facilitate targeted inspections by competition authorities, particularly in contexts that function as incubators for algorithmic collusion. Companies deploying such technologies also have a vested interest in embracing self-regulation, recognizing their broader societal responsibilities regarding potential harms stemming from algorithm deployment. In this respect, non-financial reporting obligations directed towards investors and other stakeholders could be contemplated. Put differently, preventive and monitoring measures adopted by firms may contribute to establishing a form of social licence to operate.

For market supervisory authorities, four primary challenges emerge.

- First, the **effectiveness of their enforcement activities** depends fundamentally on the availability of robust internal resources and technical capabilities.
- Second, **detecting and characterizing algorithm-driven anticompetitive practices**—particularly those involving pricing algorithms—as infringements within an effects-based legal framework necessitates procedural adaptations. These include expedited investigatory timelines (such as interim measures to prevent irreversible market harm), potentially shifting the burden of proof regarding anticompetitive effects onto implicated undertakings in certain cases, and employing flexible instruments in investigatory triggers and sanctioning powers—whether in merger control procedures or in the design of remedies adjustable according to specific circumstances and the cooperation exhibited by involved firms.
- Third, as previously emphasized, **ex post enforcement by competition authorities** becomes significantly more effective when supported by an ex ante regulatory framework that facilitates subsequent procedural implementation. For example, obligations regarding the retention and disclosure of highly granular data, although imposing compliance costs on firms, enhance the deterrent effect of enforcement while simultaneously strengthening legal certainty for regulated entities.
- Fourth, and in the same vein, a **light-touch or differentiated regulatory approach** should be prioritized. The European AI Act provides a useful model, differentiating obligations imposed on firms according to the associated level of risk. A similar rationale underlies the draft reform of the European Commission's guidance on exclusionary abuses—initially published in February 2009

and revised in August 2024—which introduces a graduated enforcement framework based on the severity of potential competitive harms.

Practices highly likely to produce irreversible market harm, such as algorithmic strategies with a significant probability of leading to parallel conduct or consumer manipulation, may warrant outright prohibition. Conversely, other practices that pose substantial challenges to ex post detection or assessment may require data retention and disclosure obligations, or even trigger a reversal of evidentiary presumptions when evaluating net competitive effects.

A central challenge resides in ensuring a coherent interplay between ex ante and ex post interventions: ex ante regulatory tools should remain narrowly focused on preventing irreversible harms and be specifically designed to facilitate accurate and timely ex post assessment of competitive effects.

6. Conclusion

To conclude, algorithms have fundamentally transformed the nature and texture of unilateral market conduct. Antitrust authorities must therefore adapt by examining micro-level pricing strategies rather than relying solely on aggregate, market-wide outcomes. They need to remain vigilant regarding exclusionary tactics that may not be immediately apparent from high-level financial metrics but become clearly visible upon detailed, algorithmic-level scrutiny. In other words, regulatory and competition authorities must ensure that sophisticated algorithmic processes do not serve as a shield for anti-competitive practices that firms could not legally execute through traditional means.

To effectively respond to these evolving challenges, competition agencies must modernize both their legal standards and investigative techniques. Emphasizing greater transparency in algorithmic decision-making processes, enforcing rigorous disclosure and reporting obligations, and encouraging proactive internal oversight can help pre-emptively address potentially anti-competitive outcomes. Moreover, continued research collaboration between competition authorities, the private sector, and academia is crucial to deepen our understanding of the implications of algorithm-driven practices, fostering evidence-based regulatory adjustments. Ultimately, such strategic enhancements in oversight capacity will not only preserve market contestability and fairness but will also strengthen public confidence in the digital economy.

References

Abada, I., Lambin, X. and Tchakarov, N. (2024). *Collusion by mistake: Does algorithmic sophistication drive supra-competitive profits?* European Journal of Operational Research, 318(3): 927-953

Autorité de la concurrence & Bundeskartellamt. (2019). *Algorithms and competition: Joint report.* Paris & Bonn: Authors.

Assad, S., Clark, R., Ershov, D., & Xu, L. (2024). *Algorithmic pricing and competition: Empirical evidence from the German retail gasoline market. Journal of Political Economy*, 132(3).

Bougette, P., Budzinski, O. and Marty, F. (2022), *Self-Preferencing and Competitive Damages: A Focus on Exploitative Abuses*. The Antitrust Bulletin, 67(2):190-207, June.

Bougette P., Budzinski, O. and Marty, F. (2024). *In the light of dynamic competition: should we make merger remedies more flexible?* European Competition Journal, December, htps://doi.org/10.1080/17441056.2024.2440228

Bougette, P., Budzinski, O. and Marty, F. (2025). *Ex-ante versus Ex-post in Competition Law Enforcement: Blurred Boundaries and Economic Rationale*, International Review of Law and Economics, 82, June. https ://www.sciencedirect.com/science/article/abs/pii/S0144818825000201

Brown, Z. Y., & MacKay, A. (2021). *Competition in pricing algorithms* (NBER Working Paper No. 28860). National Bureau of Economic Research.

Calvano, E., Calzolari, G., Denicolò, V., & Pastorello, S. (2020). *Artificial intelligence, algorithmic pricing, and collusion. American Economic Review, 110*(10), 3267–3297.

Canadian Competition Bureau. (2025). *Algorithmic pricing and competition: Discussion paper.* Government of Canada.

Cheng, T.K. and Nowag J. (2023). *Algorithmic Predation and Exclusion*, University of Pennsylvania Law Review, 25: 41-101.

Court of Justice of the European Union. (2016). *Eturas UAB and Others v. Lietuvos Respublikos konkurencijos taryba*, Case C-74/14 (Judgment of Jan. 21, 2016).

de Marcellis-Warin, N., Marty, F., Thelisson, É., & Warin, T. (2022). *Artificial intelligence and consumer manipulation: From consumers' counter-algorithms to firms' self-regulation tools. AI and Ethics, 2*(2), 259–268.

de Marcellis-Warin, N., Marty, F. & Warin, T. (2025). *Réglementer l'intelligence artificielle sur la base des risques. Perspectives économiques et éthiques.* Revue Economique, 76(1), pp.87-114.

Marty, F. (2025) *Algorithmes de prix et traitement des risques de collusion anticoncurrentielle*, Revue de l'OFCE, 188, pp.99-132.

Marty F. & Warin T. (2023a) "Coordinated Anticompetitive Practices Based on Algorithms", in Marciano A. and Ramello G.B., eds, *Encyclopaedia of Law and Economics*, Springer, New York, https://doi.org/10.1007/978-1-4614-7883-6_818-1

Marty F. & Warin T. (2023b) "Algorithm-Based Anticompetitive Unilateral Practices", *in* Marciano A. and Ramello G.B., eds, *Encyclopaedia of Law and Economics*, Springer, New York, https://doi.org/10.1007/978-1-4614-7883-6_791-1

Marty, F., & Warin, T. (2023c). *Multi-sided platforms and innovation: A competition-law perspective. Competition & Change, 27*(1), 184–204.

Marty F. & Warin T. (2024) *Algorithmes de prix et signaux collusifs : approches économique et concurrentielle*, Revue française d'économie, volume XXXIX, n°2, octobre :193-245.

Marty, F., & Warin, T. (2025). *Deciphering algorithmic collusion: Insights from bandit algorithms and implications for antitrust enforcement,* Journal of Economy and Technology, 3, November, 34-43

Mouton, J. and Rottembourg, B. (2024). A*uditing the Ranking Strategy of a Marketplace's Algorithm in the Frame of Competition Law Commitments with Surrogate Models: The Amazon's Buy Box Case*. GREDEG WP, 2024-37, http://195.220.190.85/GREDEG-WP-2024-27.pdf

Nazzini, R. & Henderson, J., (2024). *Overcoming the Current Knowledge Gap of Algorithmic "Collusion" and the Role of Computational Antitrust*, Stanford Computational Antitrust, vol 4., https://law.stanford.edu/wp-content/uploads/2024/02/Algorithmic-Collusion.pdf

New York State Legislature. (2023). *General Business Law § 1909: Transparency in personalized pricing* (Chapter 231, Laws of 2023).

OECD. (2017). *Algorithms and collusion: Competition policy in the digital age.* Paris: OECD.

Tirole, J. (2023). Competition and the Industrial Challenge for the Digital Age. *Annual Review of Economics*, 15:573-605. https://doi.org/10.1146/annurev-economics-090622-024222

UK Competition & Markets Authority. (2018). *Tackling the loyalty penalty* (Response to the super-complaint by Citizens Advice). London: CMA.

UK Competition & Markets Authority. (2021). *Algorithms: How they can reduce competition and harm consumers.* London: CMA.

United States District Court (W.D. Tenn.). (2023). *In re RealPage, Inc. Rental Software Antitrust Litigation (No. II)*, MDL No. 3071 (Consolidated Class Action Complaint).