INVISIBLE HANDS OR DIGITAL MANIPULATION?
REIMAGINING ANTITRUST IN THE ALGORITHMIC AGE

ABSTRACT

The arrival of algorithmic pricing and consumer profiling signifies a sea change for the digital marketplace in terms of competition and regulatory dilemmas. This paper reviews the new ways in which machine-learning algorithms in algorithmic pricing set tailored prices for individual consumers that exploit vast datasets of behavioral and individual consumer online/offline data. Algorithmic pricing and profiling technologies have the potential to maximize economic efficiency and increase the availability of tailored, customized offerings, at the same time they raise difficult issues of fairness, discrimination, and the exploitation of consumers.

A thorough analysis of the enforcement gaps under U.S. and EU anti-trust enforcement demonstrates that the existing anti-trust regime and regulatory structure have little experience with self-governing, autonomous algorithmic behavior. A deeper issue is how dominant firms markedly leverage data asymmetries to develop barriers to entry that bolster their market platform, and a broader concern should focus on how some bloc of consumers get marginalized or neglected due to the presence of exploitive dominant firms. The paper then steps back and consider the social and ethical consequences of less transparent profiling systems in which there is little autonomy for the consumer and privacy protection is often outweighed by growth objectives. Given these challenges, the research emphasizes the urgency of developing new regulatory tools - such as algorithmic audits, mandatory transparency, and cooperation across agencies in terms of competition and data protection agencies.

I. INTRODUCTION

In the expansion of the digital marketplace technology firms have now started selling products and services in the marketplace by means of machine learning algorithms and pricing algorithms backed by a personal data set for consumers. These technologies are intended to create individual-level price manipulations. While these technologies can be understood as the most explicit form of price discrimination, they instigate a new peril, evolving into the scenario of algorithmic collusion - algorithms are now the price-setters without any human involvement while still setting supra-competitive prices and harming consumer welfare. So, these forms of tacit coordination raise the question of Group Boycotts under traditional anti-trust law, which requires proof of some agreement or affirmative communications between, at least two, competing firms, or perhaps the classic Cartel case in which competing firms also compete against the customers; i.e. hybrid anti-competitive practices.

The threat stems from the economic theories and simulative studies that show the prospects for algorithmic collusion, and in addition, studies find that individually learning pricing algorithms, perhaps also self-learning algorithms will converge more quickly into collusive equilibria, even though, ex ante, none of them intended/explored price fixing, which may occur, for example, in highly transparent markets, or if firms engage and re-engage many times. In addition, algorithms very rarely outperform one another when trained on very similar data sets, and thereby they will correlate their price responses, and perhaps this is one way pricing aligns itself quietly through similar algorithms, without the involvement of humans, and is mistakenly believed as being a conspiracy.

Legal authorities dealing with anti-trust issues are struggling to coordinate enforcement against algorithmic collusion using a lens of traditional concepts. In the U.S., the anti-trust enforcement process ultimately must hinge on an agreement under the Sherman Act, which leaves a large enforcement gap around coordinated pricing using machines. Proposed legislation has tried to close the gap by stipulating that simply using similar algorithms to price should be treated as "presumptive evidence" of collusion. Within the European Union a distinct literature and practices of enforcement are developing to use the concept of "concerted practice" to encompass the algorithmic facilitation of coordination among competitors.

The profiling of consumers, along with various data such as user behavior, physical location, and online activity, is a means of increasing competition risk by leveraging an equal and opposite lever. This means that firms can customize offers based on individual preferences, and at the same time, use data to solidify the position of category leaders using barriers to entry and the network effect. The impact or deep influence on consumers is generic and multiplicative. For example, algorithmically-based price discrimination can benefit consumers as it increases the chance of individual consumers receiving discounts. However, algorithmic collusion can benefit conspiracy by raising prices to an extent that negatively impacts the entire consumer mass. Ultimately, the profiling of consumers will use data in a way that foster contempt for consumers by all that have industry insider information, create opportunities for suspect or opaque pricing, and constrain human choice arising from the procurement of digital solutions.

Fast developing competition enforcement tools are one agenda item in the wake of the increasingly algorithmic systems shaping the world. These systems are complex and, often mysterious to the rest of us, and they drive self-learning models. Some legal scholars have hypothesized that some kinds of algorithmic behavior might be considered a "plus-factor" of collusion, and certainly ex ante merger assessments should be examining mergers where firms have data assets of substantial

value.[1] Perhaps this is an occasion for regulators to shine a light more broadly on alternative investigatory methods, like algorithmic reviews and mandated transparency, that would engage cooperation between competition and data protection authorities to counter the dual harms of algorithmic collusion and consumer profiling in the data rich economy.

II. ALGORITHMIC PRICING AND CONSUMER PROFILING IN DIGITAL MARKETS

Digital markets have changed irrevocably over the past twenty years due to enormous activity in the field, systemic access to data, improvements in machine learning algorithms, and accelerating computational power. Two important new areas of activity are algorithmic pricing, a dynamic pricing mechanism that automatically updates price based on real-time data input and predictions; and growing methods of consumer profiling.[2] Consumer profiling is important for firms to understand their offering better; sell targeted consumers; and comprehend predicted consumer behaviour with enormous amounts of personal and behavioural data. The stimulus and redefinition of competition, new firm strategies, and challenges with new form of regulatory and ethical concerns.[3]

Price customization or price discrimination is one of the major Moves from the norm of a general price that algorithmic pricing has already begun to facilitate. There is a continuous pattern of firms engaging in a type of first degree price discrimination and wanting to charge every individual consumer the highest amount that each consumer is willing to pay.[4] Firms will use broad consumer profiling to determine price level based on the extensive online data of each consumer's behavioral and browsing history, historical searches (search engines and social media), the specific type of device the consumer is using (for example, a phone vs. a tablet), and if applicable, sometimes the consumers actual location matters.[5] The informational data allows firm algorithms to gather details about consumer's income level, brand loyalties, price sensitivities, and intentions which help sellers in setting the right price level. At the same time, it guides buyers toward purchasing products, or services while also boosting the seller's profit.[6]

Such power has consequences that can reach long and wide. That is, it could actually increase economic efficiency since some firms perform the service more economically and broadly than

---

1 Maurice E. Stucke and Ariel Ezrachi, 'Data Assets and Merger Review: Antitrust Implications of Algorithmic Pricing' (2024) 2024(4) University of Tennessee Legal Studies Research Paper No. 478/2024

2 Ariel Ezrachi and Maurice E Stucke, 'Artificial Intelligence & Collusion: When Computers Inhibit Competition' (2017) 2017(3) Oxford Legal Studies Research Paper No 18/2017

3 Salil K Mehra, 'Antitrust and the Robo-Seller: Competition in the Time of Algorithms' (2016) 100 Minnesota Law Review 1323

4 Ibid

5 Maurice E Stucke and Ariel Ezrachi, 'How Big Data and AI Can Collude to Hurt Consumers' (2017) Harvard Business Review

6 OECD, 'Algorithms and Collusion: Competition Policy in the Digital Age' (2017)

the others that would sell the service with a uniform price. Personalized pricing creates huge issues concerning fairness, discrimination, and manipulation of consumers. Consumers may not have conscious awareness that one consumer is charged and pays more than the next person, thus eroding trust in the pricing and in the transparency of pricing.[7]

The digital marketplace has dramatically changed over the last twenty years not just in terms of the sheer volume of data available and advancements in machine learning applications, but also computing has become unbelievably dynamic in terms of computing power. A particularly important example of this type of data-based power is algorithmic pricing—this is a data-heavy price setting method where pricing is based, at least in part, on real-time and predictive analytics. Further, profiling methods of firms and consumers are becoming increasingly relevant to firms that want to customize pricing approaches through price discrimination utilizing behavioral knowledge that has emerged out of large quantities of personal and behavioral data.[8] So the actual environment of competition has changed, firms have changed their strategic approaches which present new regulatory and ethical dilemmas. Importantly, the largest change that algorithmic pricing creates is that price becomes personal or differentiated rather than standardized price, creating more ability to practically achieve first degree price discrimination (i.e., charge each consumer the maximum they are willing to pay).[9] Identifying opportunities inherent in the asymmetries between the consumer's information regarding personal profile data gleaned from their online activities, their past online searches, social network linkages, and even their current location can happen! Algorithms are able to scrape that information which amounts to, estimated income levels, brand loyalty, price sensitivity, intention, patterns assumed by the consumer so that sellers can find a price to pitched to consumer.[10]

Such capabilities can have significant effects. To wit, algorithmic pricing creates more economic efficiency as a business can make available a product or service to more subsets of consumers as well as to consumers who would not otherwise purchase that particular product or service at all given a particular standard price. However, while personal pricing can price consumers better, the impacts regarding fairness, discrimination, and manipulation of consumers is incredibly serious. Consumers may not be aware that one consumer may be paying more than another consumer which undermines fairness and trust; transparency in pricing practices abandoned.[11]

---

7 Ibid
8 UN Special Rapporteur on Freedom of Expression, 'Surveillance and Human Rights in the Digital Age' (2022)
9 European Data Protection Supervisor (EDPS), 'Algorithms and Human Rights: A Study on the Implications of Advanced Analytics and AI Systems' (2020)
10 Ibid
11OECD, 'Competition Policy for the Digital Era' (2019) https://www.oecd.org/competition/competition-policy-for-the-digital-era.htm (accessed 5th July 2025)

Algorithmic pricing is accomplished through complex machine learning models generally through Reinforcement Learning or Deep Learning based methods. These models have a very high level of efficiency by automating pricing at a real-time basis and available to the user. The algorithmic pricing systems analyze large data inputs from many. Big data in pricing systems can include past sales history, competitor pricing, industry market research trends, or consumer data trends.[12] Algorithmic pricing could result from the real time price changes and create price changes based on big data. E-commerce sites for example can create a price point or change one based on previous action, the total time on a page by second, or the type of device being used (ex: charge more for user action using a 'premium' type device). OECD, 2019 indicated that systems today can change pricing hundreds of times a day, a feat possible through automation that is impossible for humans to do.[13]

Price discrimination also relates to large groups of consumers, firms group consumers into segments of consumers by similar characteristics (i.e., Purchasing power, brand) that can use the price discrimination in second or third-degree manner. Firms utilize dynamic pricing based on consumer demand, and consumer demand at the time of day, which is location dependent, to discriminate against consumer groups.[14] For example, airlines and ridesharing companies have used dynamic pricing for some time. The consumer profiling model of attributes was briefly mentioned in a Journal of Economic Perspectives publication entitled: Consumer Profiling: The Data-Driven Engine, (2021), (special issue) where similar price discriminations were occurring in retail, hospitality, and some forms of digital subscriptions made possible by big-data, cloud computing, algorithmic analysis.[15]

In our essence, algorithmic pricing commences with consumer profiling based on personal and behavioral data which can be multifaceted and innumerable. This assorted data can include browsing history, consumption data, consumption of social media, geospatial location information, and relevant biometric data, and in some cases can include things can't even be named.[16] It is not to be implied that companies cannot at least conduct some basic analysis when conducting sophisticated analytics (such as natural language processing and sentiment analysis) to infer consumer preferences and willingness to pay. In 2023, a report by McKinsey suggests that companies using a consumer profiling approach in decision-making take account of particulars of

---

12 Federico Etro, 'Algorithmic Pricing and Competition: A Review of the Literature' (2021) 13(2) Journal of Industrial and Business Economics 217

13 Ibid

14 Florian Wagner-von Papp, 'Algorithmic Collusion and the Need for a More Dynamic Antitrust' (2020) 83(3) Modern Law Review 1

15 Ibid

16 OECD, 'Price Discrimination and Competition' (2016) https://www.oecd.org/daf/competition/price-discrimination.htm

pricing and marketing decisions with respect to improperly profiling and can obtain margin improvement by as much as 15 percent.[17] That said consumer profiling does raise a multitude of ethical issues in its application. The largesse of how data is collected, to frequently no modelling for consumers practice using their data lends to the opacities. Pew Research Center's 2022 report, found 79% of consumers feel their consumer agency has been diminished in relation to how companies gather data and use data, and has previewed distrust with digital markets.[18] Furthermore, profiling may ensure that some inequities are entrenched in the system wherein under-represented consumer communities may be subject to predatory pricing, or terms discussed generally in the academic literature.[19]

A. Market Dynamics and Competing Media

Algorithmic pricing and consumer profiling are changing the way competition functions in digital markets. They can create competitive markets for small firms looking to compete with larger established firms with good data practices, and they allow "big data" and "big computing" tech firms to act as monopolists with their valuable data. In this scenario if a firm has significant information asymmetries or is "locked" into a constellation of sub-standard or unsustainable firms, due to network effects or economies of scale, then they will have a clear incumbent advantage versus a small firm new entrant. Based on the use of algorithmic pricing will indirect tacit collusion emerge? While the algorithms and the market will code very different data to learn pricing strategy, the pricing algorithms for a number of firms might converge on an independent yet ex-post profitable pricing strategy irrespective of coordination.[20] A 2020 study in the American Economic Review with simulations supports this notion by demonstrating how reinforcement learning algorithms can arrive at collusive outcomes almost irrespective of direct conversation in oligopolistic markets. In the literature it has been referred to as "algorithmic collusion" and it raises potential new challenges for anti-trust enforcement which may previously have considered potential harm in terms of explicit agreements or coordinated conversations.[21]

B. Social and Ethical ramifications

In addition to competitive challenges, algorithmic pricing and consumer profiling generate ethical and social issues. If a consumer finds out that they were charged more for a given product or service than another individual, they may perceive their prices unfairly and their trust in the markets

---

17 Ryan Calo, 'Digital Market Manipulation' (2014) 82(4) George Washington Law Review 995
18 Pew Research Center, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information' (2019)
19 FTC, 'Big Data: A Tool for Inclusion or Exclusion?' Understanding the Issues (FTC Report) (2016)
20 Calo, 'Digital Market Manipulation' (n 16)
21 European Commission, 'A New Era for Consumer Policy: Empowering Consumers to Benefit Fully from the Digital Transition' (2020)

is likely to be diminished.[22] Not only is this a challenge, but they could also find out that the algorithms representing their personal data is based on unethical information, and other applicants similarly experience the inequity of algorithms more generally, marginalised consumers may be even more disproportionately impacted by pricing algorithms. Social considerations also include privacy concerns. Consumer identification systems, which require massive data collection consumers haven't consented to, infringe on consumer autonomy and rights of ownership of their information.[23] As a result, we have seen jurisdictions, such as the European Union, encourage frameworks, the General Data Protection Regulation (GDPR), which implement very detailed and prescriptive measures for data collection and processing; however, enforcement is consistently uneven. In addition, because jurisdictions have unique laws governing data protection, companies find it easy to develop a landscape of data protection regulations that will permit certain behaviours by using the different standards as non-binding best practices.

The beginning of algorithmic pricing and consumer identification can usher in a new era for digital markets. Algorithmic price setting and consumer identification make it open to a firm to develop pricing regimes that in some manner increase allocative efficiency in the overall market. However, these systems may open companies to allegations of unfairness, discrimination, and tacit collusion.[24] As these markets continue to evolve, regulators, firms, and consumers have to stand in support of balancing the ability to innovate and gain efficiencies from algorithmic pricing and consumer identification systems against maintaining a fair market and competition. The following chapter reviews some of the legal and regulatory constructs with which a response has been mounted to the growth and use of these technologies, namely anti-trust enforcement and data protection.[25]

III. ENFORCEMENT OF ANTI-TRUST IN THE AGE OF ALGORITHMIC COLLUSION

In the zeitgeist of rapid technological changes, machine learning and artificial intelligence (ML/AI) have actually thrown the competitive environment into chaos in nearly every industry by way of installing myriad pricing algorithms or "machine-pricing" systems that use big data for price decisions. Pricing algorithms have really stirred up a storm when it comes to the potential for anticompetitive behavior, like algorithmic collusion. Algorithmic collusion can be implicit whereas traditional collusion often requires an explicit agreement; in this sense, algorithmic collusion can occur quietly as algorithms independently learn and adjust themselves to each other's pricing and

---

22 Ibid
23 UK Information Commissioner's Office (ICO), 'Explaining Decisions Made with AI' (2020)
24 Dana Polatin-Reuben and Joss Wright, 'An Internet with BRAS: De-Anonymising Users Through Automatic Network-Level Profiling' (2017) 16(3) Surveillance & Society 312
25 Jamie Luguri and Lior Strahilevitz, 'Shining a Light on Dark Patterns' (2021) 13(1) Journal of Legal Analysis 43

strategy to reduce competition.[26] An inventory of issues in anti-trust enforcement is posed by algorithmic collusion; a discussion of the law and economics relating to it; and possible solutions for safeguarding highly competitive markets in the digital age will be undertaken.[27]

Algorithmic pricing bridges the world of prices by creating changes in prices quickly and based temporally on perceived information of market conditions, consumer behavior, and pricing of a competitor. These systems and algorithms form proprietary price maximizors embedded in the AI, which, through real-time adjustments to price, maximize profit in ways and on a scale never before possible.[28] Sellers in different sectors such as e-commerce, real estate, hospitality, and transportation have started applying algorithmic pricing in their operations to better streamline them and to make them more responsive in real time. Alongside these are risks, which, when priced algorithmically, may produce unacceptable anticompetitive results. The set-up allows a capacity for high datasets and lightning-fast response to market condition changes, hence it almost acts like a level of coordinated conduct (or pricing), similar to a cartel but without any human concert.[29] If this were ever to arise, serious bullish issues would arise for anti-trust and competition laws, which are historically focused on having to provide proof that an agreement to act or concert is mostly supported by written statements or other forms of construct that can establish a chain whereby liability can be attributed.

A. Understanding Algorithmic Collusion

There are different ways of engagement in algorithmic collusion, and these can create difficulties for anti-trust enforcement:

1. <u>Explicit Collusion using Algorithms</u>: Competitors can use algorithms for explicit conduct, such as algorithms that allow for sharing sensitive pricing information through a common algorithm. For example, *U.S. v. David Topkins (2015)*[30] involves competitors using algorithm-based software to coordinate changes to prices for on-line sale of posters, and resulted in a criminal conviction for price-fixing under Section 1 of the Sherman Act.

2. <u>Tacit Collusion using Parallel Conduct</u>: Algorithms can independently learn to undertake pricing strategies that result in supra competitive prices without any direct communication of a pricing intention amongst competitors.[31] Laboratory experimental studies, such as those using Q-learning algorithms in market simulations, have shown that these algorithms

---

26 Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880
27 Woodrow Hartzog and Frederic Stutzman, 'The Case for Online Obscurity' (2013) 101 California Law Review 1
28 Ibid
29 Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54 Journal of Economic Literature 442
30 United States v David Topkins, No CR 15-00201 (N.D. Cal.2015).
31 OECD, 'Data-Driven Business Models and Competition' (2020)

can reach collusive equilibria, even when they have not communicated with one another. This tacit collusion presents real problems for current anti-trust laws and policy, as it lacks the "agreement," or "concerted practices," prescribed by rules such as Article 101[32] of the Treaty on the Functioning of the European Union (TFEU) or Section 1[33] of the Sherman Act.

3.   <u>Hub-and-Spoke Collusion</u>: In this variation, competitors produce sensitive information that is formed into recombineable content by a third-party algorithm provider. As a result, the algorithm makes recommendations about volumes of activity or prices that connect competitors' patterns of interactions or strategies. The RealPage case from the U.S., in which landlords employed a centralized pricing algorithm in order to raise rental prices, is representative of this model. The U.S. Department of Justice (DOJ) and Federal Trade Commission (FTC) argue that such arrangements develop outmoded price fixing agreements by eliminating the mechanism of independent thinking in the market.

4.   <u>Autonomous Algorithmic Collusion</u>: The most troubling case involves a future scenario of self-learning algorithms that identify and act on collusive strategies without human involvement. Preliminary research indicates that reinforcement learning algorithms can learn to set high prices without communicating with other agents, with the greatest divisive results in concentrated markets with limited constraints on price.[34] This raises broad questions about whether the behavioral restrictions of anti-trust law would be able to confront conduct no longer primarily organized or implemented by humans driven by autonomous systems.

D. Legal Issues

Anti-Trust laws in the world, including the US Sherman Act and EU competition law, are geared towards human collusion and monopolistic practices, and algorithmic collusion presents new challenges that challenge both existing definitions of collusions and violations of competition law:

-    <u>Definitions of an "Agreement"</u>: Most anti-trust law requires proof of an agreement or concerted action before Section 1[35] Sherman Act or Article 101[36] TFEU liability is established. Proving an "agreement" in tacit algorithmic collusion cases when the algorithms create the same collusive outcomes independently is all but impossible. In the

---

32 Art. 101 TFEU
33 Sherman Antitrust Act 15 USC 1 (1890)
34 Cristina Caffarra and Oliver Latham, 'The Economics of Digital Markets: A Practitioner's View' (2020) 2(1) Journal of Antitrust Enforcement 123
35 Ibid
36 FTC, 'Protecting Consumers in the Next Tech-ade: A Report on the Federal Trade Commission's Tech-ade Hearings' (2009)

Eturas case (2016)[37], the European Court of Justice provided a tacit agreement could be established where there was knowledge of a common price-restriction, but an autonomous algorithmic action does not fulfill any "knowledge" or "purpose".[38]

-   Attribution of Liabilities: If algorithms function in an autonomous capacity, determining liability, the entity, developer of the algorithm, or provider of the third party is complicated as well. Current legal frameworks and courts are ill-equipped to address and allocate responsibilities arising from a self-learning system when firms assert that they were unaware of any collusive outcomes.

-   Identifying Collusion: Identifying algorithmic collusion will require advanced technology to assess pricing patterns and algorithmic behaviors, and competition agencies may lack the resources and technical capabilities to identify collusive results and relationships even with proprietary algorithms. Also, the algorithmic game may lead to complex pricing that could be difficult to disentangle from normal, competitive, pricing behavior.[39]

-   Establishing Ant-itrust Injury and Damages: Proving anti-trust injury and damages in cases involving algorithmic collusion is complicated by the absence of a consensus on whether algorithmic pricing leads to supracompetitive prices. For example, in *Duffy v. Yardi Systems*,[40] the DOJ's argument that using a third-party algorithm to drive price starting points was price-fixing still did not create a method to measuring the actual harm to consumers, using a created "but-for" world where no algorithms existed, which would be complicated given the nature of pricing algorithm dynamics.

E. Economic Considerations

From an economic perspective, algorithmic collusion blurs the line between rational pricing and anticompetitive conduct. Algorithms can facilitate efficiency by permitting firms to be adaptive to changing market conditions, but they may also facilitate stability in collusive equilibria by minimizing uncertainty and instability associated with interdependent pricing.[41] Bandit algorithm studies have proposed that algorithms can reach supracompetitive prices faster than humans, particularly in concentrated markets with few competitors, just from the probability of agreement. Yet, empirical examples of algorithmic collusion are almost nonexistent. While experiments can illustrate the collusion potential in a laboratory setting, there are few real-world examples; we do

---

37 Eturas UAB and Others v Lietuvos Respublikos konkurencijos taryba (Case C-74/14) EU:C:2016:42.
38 Ibid
39 Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18
40 Duffy v Yardi Systems Inc, No 2:21-cv-01702(WD Wash 2021)
41 Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671

not have a measurement of the frequency of the occurrence of such behavior. Furthermore, some scholars have argued that pursuing the study of algorithmic collusion could detract from other important anti-trust issues, such as monopolization or exclusionary conduct, where anti-trust agencies or consumers could more easily show harm.[42]

F. Enforcement Actions prevalent

Anti-trust authorities across the globe are trying to meet algorithmic collusion challenges[43]:

- United States: DOJ and FTC have taken a firm position by filing statements of interest in cases like RealPage and Duffy v. Yardi Systems,[44] and by arguing that an agreement to use common pricing algorithms is a per se violation of the Sherman Act. The DOJ's "Project Gretzky" demonstrates a commitment to hiring data scientists and AI experts to further its enforcement. Legislative proposals, such as the Preventing Algorithmic Collusion Act (introduced in 2024), clarify the definition of an agreement to close loopholes by presuming price-fixing when competitors share sensitive information via algorithms and requiring disclosure of algorithmic pricing.

- European Union: The EU has had fewer cases directly addressing algorithmic collusion, but the OECD and EU regulators have recognized most existing legal frameworks do not even contemplate autonomous tacit collusion as something capable of being caught on an extensive scale. The EU is discussing changes to "agreement" or "concerted practice" for the purposes of tacit collusion to subsequently include coordination by algorithms, though no reforms have been implemented.

- Other Jurisdictions: Some authorities in jurisdictions such as India and ASEAN are starting to address algorithmic collusion in digital markets and stressing the need for regulators to have an effective regulatory tool to promote consumer welfare.

Algorithmic collusion is a new test for anti-trust enforcement that poses challenges concerning traditional legal and economic analysis. While algorithms provide potential efficiencies in markets, their ability to enable tacit collusion without any express communication risks competition and harms consumers. The initial enforcement efforts being undertaken around algorithmic collusion-particularly in the United States-have illustrated a growing recognition of the challenge to enforce anti-trust law, but there remain invaluable gaps in identifying, assigning liability for, and designing remedies for collusion that enables algorithmic collusion.[45] By prioritizing a proactive approach

---

42 Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs 2019)
43 Maurice E Stucke and Ariel Ezrachi, 'How Big Data and AI Can Collude to Hurt Consumers' (2017) Harvard Business Review
44 Duffy v Yardi Systems (n 39)
45 Niamh Dunne, 'Fairness and the Challenge of Platform Regulation' (2020) 79(3) Cambridge Law Journal 493

that preserves the benefits of innovation in technology, including transparency, compliant-by-design, and targeted remedies, regulators can reduce the risks associated with algorithmic collusion.[46] As the digital economy continues to develop, the challenges posed by algorithmic collusion will remain real- continued examination and discussion between the regulators, companies, and academics will be necessary to ensure that anti-trust law is fit for purpose when it comes to algorithms.

IV. CONSUMER PROFILING AND ITS IMPACT ON COMPETITIVE FAIRNESS

Consumer profiling is the process in which an organization collects, analyzes, and utilizes data to create comprehensive versions of consumer patterns, preferences, and demographics. Organizations use this process in order to enhance their marketing, provide an improved customer experience, and create greater efficiencies. Organizations access and combine data from multiple sources, such as purchase history, web activity, social media, demographics, and others to develop profiles for personalized offerings.[47] The implications of consumer profiling framed in terms of the level of competitive fairness - especially with respect to how it can affect market dynamics - as well as the issue of consumer trust, raises questions about the manner in which utilize it.

A. Technologies of Consumer Profiling

Distributing and compiling electronic databases as a luxury, current technology continues to take advantage of developing technologies as sophisticated data sources for consumer profiling, including big data, data analytics, machine learning, and artificial intelligence in the machine to read and analyze large volumes of data to find patterns and predict consumer preferences and behavior.[48] For instance, e-commerce platforms make recommendations based on their browsing histories or clickstream data, and retailers have used loyalty programs to develop profiles and examine local purchasing trends. Similarly, third-party data aggregators can compile profiles by adding outside information about a person's credit scores or social media interactions as they compile consumer profiles. As a result, businesses will be able to more precisely delineate consumers into smaller segments of target market segments and create advertising and promotional elements specifically designed for those groups. Because some of the powerful information available at the individual levels of profile detail will allow exceptionally precise targeting strategies by excluding certain consumer segments or a smaller competitor. [49]

B. Consequences for Competitive Fairness

---

46 Ibid
47 European Data Protection Board (EDPB), 'Guidelines on Automated Individual Decision-Making' (2020)
48 Ibid
49 European Data Protection Supervisor (EDPS), 'Algorithms and Human Rights: A Study on the Implications of Advanced Analytics and AI Systems' (2020)

Competitive fairness implies that businesses are competing in an equitable competitive space, where one business does not receive unwanted advantages over other businesses based on unfair practices. Consumer profiling creates competitive fairness concerns in three ways:

i. Dominance and barriers to entry

Large companies have the potential to buttress their market position through consumer profiling; because they are able to leverage large sets of data much more effectively than small-to-medium-sized enterprises, savvy decision-makers in the large firms can employ sophisticated decision-making algorithms that can respond to consumers' explicit and context prevailing preferences. Therefore, the large firms eventually have high confidence regarding consumers' purchasing patterns and can offer better consumer experiences which the small firms cannot offer according to their poor data application mechanisms and inevitably data coverage which tends to be limited from suppliers.[50] However, the ability to provide distinct consumer experiences suggests asymmetrical competition because the small firms cannot leverage significant resource expenditures to conquer proprietary profiling capabilities to be able to predict the experiences their customers undergo.[51] For example, a small retailer cannot compete for personalized recommendations at the scale of a global e-commerce giant. This almost undefined product experience may inhibit new product development and subsequently inhibit diversification in any one market segment.

ii. Price Discrimination and Consumer Exploitation.

The dynamic pricing aspect of consumer profiling can be manipulated to elicit price differences based on the consumer, in ways that work in conjunction with consumer data types that create what some would refer to as "super pre-test price sensitivity."[52] That is, to maximize firm profits, firms can extract even more from consumers if they manipulate access to customer data, and this could be done in a way that profiled influential consumers, who may be completely unaware they have been purchased at an excessive price. For example, a consumer profiled as full "price insensitive," may pay a much larger price, than a consumer profiled as only "price sensitive," for the same consumer good or service. Firms might also be able to engage in discriminatory practices toward vulnerable populations, which further calls into question their ethical commitments. Finally, firms without profiting capabilities, or consumer-level data, would only be held accountable to consumers who valued their pricing as fairness, not price discrimination, which hides fair market actor's behaviors.

---

50 Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI' (2019) 20 Columbia Business Law Review 494
51 Anu Bradford, 'The Brussels Effect and Global AI Regulation' (2022) 2(1) European Journal of International Law 37
52 Ibid

<u>iii. Concerns of Privacy</u>

The requirement for enormous amounts of data to create profiles of consumers usually involves a violation of consumer privacy, resulting in distrust. Consumers have little or no idea how much of their data is collected, shared, or sold. There have been a series of data missteps over the past few years and most recently, data breaches of enormous reach, which placed consumer use of data under a spotlight and consumers are demanding transparency and accountability.[53] Consumers possibly see profiling or the capturing of their data as an invasion of their privacy, and they may just stop using certain brands altogether and instead start using brands that, by their own preference, have significantly less aggressive means to track consumer data.[54] This also had the impact of hurting data reliant companies, but it also demonstrated a need for ethical conduct from companies with data mining steps to build data profiles for competitive advantage.

C. Regulatory Issues

The consequences of consumer profiling may invoke a wide variety of authorities at all levels of government and regulation. There are a number of frameworks to protect consumer rights, and make sure consumer profiling occurs in a fair manner. The EU provides a good example of this, though the General Data Protection Regulation (GDPR) - Google, Facebook, etc. must disclose how they collect your data and give an 'opt out' to consumers who are concerned about their personal data.[55] A similar regulatory framework, although not specifically focused on consumer profiling is present in California, the California Consumer Privacy Act (CCPA),. Both regulatory frameworks are aimed at normalizing consumer profiling across our businesses, as a result though, limits how businesses regulate, use and address their ethical concerns relating to the benefits from relating the vast amounts of profiling data obtained from these consumers.[56] The difficult aspect for all businesses with such directives will be compliance.[57] Particularly for small businesses, the cost of complying will put them at a competitive disadvantage against larger competitors.

It is up to businesses to balance personalization with consumer autonomy in the moral context. Clear practices surrounding data (e.g., strong privacy policies, opt-in consent) can help frame consumer fears about data and foster trust. Further, businesses that are serious about ethical profiling may find themselves ahead of their competitors in attracting privacy-minded consumers, and therefore encouraging fairness through market based incentives.[58]

---

53 Future of Privacy Forum, 'Algorithmic Impact Assessments: A Practical Guide' (2021)
54 Bradford, 'The Brussels Effect and Global AI Regulation' (n 46)
55 EDPB, 'Guidelines on Automated Individual Decision-Making' (n 44)
56 NYU Stern Center, 'Competition in Digital Markets: Toward a Pro-Competitive Regulatory Framework' (2021)
57 Edwards and Veale, 'Slave to the Algorithm?' (n 38)
58 AlgorithmWatch, 'Automated Decision-Making Systems in the EU: State of Play and Challenges' (2021)

Actions that can be undertaken by businesses and policy-makers towards competitive fairness include:

1. Data-sharing regimes: Support for data-sharing agreements under open data initiatives will help to achieve equity of conditions and acknowledgment of smaller business access to consumer data, which otherwise greatly depends on the larger businesses.

2. Algorithmic transparency: Legislate the profiling algorithms to be transparent so as to allow for vetting for discrimination and for ensuring fair price for consumers.

Consumer information: Consumer information on profiling is a way of promoting the conscious consumer and trust while encouraging market competition based on trust.

Consumer profiling offers great advantages in terms of personalization for the customer, operational efficiencies for organizations, but potential negative effects on competitive fairness. Large organizations can use consumer profiling to achieve or maintain a dominant market position and meet consumers' individual needs while disadvantaging smaller competitors, ultimately taking advantage of consumers through price discrimination, etc.[59] A regulated environment and ethical conventions will help to create a market where innovation and consumer trust will flourish. Regulated environments can be created that help large organizations achieve better profiling outcomes, while providing a fair dynamic market place.

V. EMERGING TECHNOLOGIES AND THE EVOLVING ENVIRONMENT OF COMPETITION LAW ENFORCEMENT

The amplification of emerging technologies, including artificial intelligence (AI), blockchain, big data analytics and digital platforms, is transforming markets all over the world. They are creating new challenges and opportunities for competition law enforcement and have fundamentally altered business models and consumer interaction with businesses. This makes it crucial for competition authorities to alter the way in which they respond to anticompetitive practises, market power and consumer welfare. This chapter will explore the connection between emerging technologies and competition law, and assess how we are seeing regulators evolve in response to new issues, while attempting to ensure innovation can continue to grow in the framework of competition law principles. The chapter will identify key issues, recent activity and potential ways for regulators to successfully enforce competition law in the digital economy.

A. Emerging Technologies and the Market

---

59 EPIC (Electronic Privacy Information Center), 'Protecting Consumers from Algorithmic Discrimination' (2021)

Emerging technologies are profoundly changing the structure and functioning of markets and giving rise to complexities that the traditional guidelines or frameworks of competition law were not intended to address.[60] Importantly, the next sections identify the main technologies that are changing these markets and how these changes are impacting competition.

B. Artificial Intelligence and Algorithmic Decision-Making

Businesses are increasingly utilizing AI and machine learning algorithms to improve pricing, tailor products and services to meet consumer preferences, and facilitate internal decision making and operational efficiencies. However, these technologies can be applied to anticompetitive practices such as algorithmic collusion.[61] For example, if competitors use pricing algorithms that have the ability to coordinate prices among them, they would obviate the need for explicit human decision-making and risk tacit collusion altogether. A 2023 OECD study observed the use of AI-driven pricing tools under controlled conditions on a public e-commerce retailer revealed higher prices resulting from the collective use of the tool, which led to attention from competition authorities.[62] Moreover, AI may worsen market concentration at a lower, more localized level by providing behemoth-sized companies the ability to create predictive analytics across large, national data sets and use them effectively in barriers-to-entry scenarios to smaller competitors. The European Commission's report regarding the 2024 Digital Markets Act (DMA) revealed that AI-driven personalization may "lock" consumers into ecosystems, and restrict single or multi-option "switching" as barrier to entry, which reinforces market power.[63]

C. Big Data and Market Power

Advertisers and new product creation increasingly harness new technology capabilities to analyze consumer data in large quantities. New product creation is supported by consumer data analytics in the same way as targeted advertising can help target customers better. Control over large data sets can entrench a position of market power if one entity controls the large data set that others depend on.[64] For example, the U.S. Federal Trade Commission's (FTC) 2025 Digital Economy Report expressed that data monopolies may reduce competition, by reducing competitors' access to useful inputs needed for innovation.[65]

A market that is data driven can also raise privacy concerns that sit at the intersection of data management and competition law. For example, in its 2024 investigation into a major social media platform, Investigatory powers and sanctions, the German Bundeskartellamt, started to have

---

60 Barocas and Selbst, 'Big Data's Disparate Impact' (n 40)
61 Center for Democracy & Technology, 'Algorithmic Transparency: End Goals and Challenges' (2018)
62 OECD, 'Price Discrimination and Competition' (2016)
63 EPIC (Electronic Privacy Information Center), 'Protecting Consumers from Algorithmic Discrimination' (2021)
64 NYU Stern Center, 'Competition in Digital Markets: Toward a Pro-Competitive Regulatory Framework' (2021)
65 US Federal Trade Commission, 2025 Digital Economy Report (FTC 2025)

concerns about the possibility that exploitative use of data-based practices can be determined as abuse of position under Article 102[66] of the Treaty on the Functioning of the European Union (TFEU).[67]

D. Blockchain and Decentralised Markets

With blockchain, we have seen the rise of a new technology that fundamentally disrupts traditional market structures, especially around financial services and supply chains, through the decentralised and public nature of cryptocurrency and blockchain. While we see blockchain enabling more competition through fewer intermediaries, both blockchain and decentralisation have opportunities and risks of their own. For example, the challenges of decentralisation can be a weakening of accountability structures and action against anticompetitive behaviour could become even more difficult.[68] The briefing on blockchain prepared by the World Economic Forum (2025) acknowledges how smart contracts as applications of blockchain, could be engineered to carry out exclusionary practices, something that requires additional regulation in respect of digital markets.[69]

E. Digital Platforms and Network Effects

Numerous digital platforms and marketplaces, contingent on the nature of the online marketplace or social media networks, benefit from network effects. Network effects refer to services that increase in value depending on the number of users using them. When network effects occur, markets can end up being winner-takes-all and we have seen examples of this kind of dynamic with organisations such as Meta, Alibaba.[70] A report issued by the UK Competition and Markets Authority (CMA) in 2024 found digital platforms also created preventable barriers to entry in the market where they had positive network effects; thus, lawmakers and regulators have been encouraged to consider ex ante regulation via frameworks, such as the DMA, to counterbalance the problems with gatekeeper businesses.

VI. CASE STUDIES

A. Google (EU, 2017–2024)

The cases brought against Google by the European Commission highlight the dynamic evolving landscape of competition enforcement. In 2017, Google was fined €2.42 billion for abuse of dominance in search as a result of placing its shopping service in a more favourable position than its competitors.[71] The 2018 matter (Android) and the 2019 matter (AdSense), however, targeted ecosystem lock in and then more exclusionary behaviour. Google was declared to be a gatekeeper

---

66 Art. 102 TFEU
67 Bundeskartellamt, 'Social Media Platform Data Investigation' (2024)
68 Future of Privacy Forum, 'Algorithmic Impact Assessments: A Practical Guide' (2021)
69 Ibid
70 Open Markets Institute, 'Amazon's Antitrust Paradox Revisited' (2021)
71 European Commission, Google Antitrust Decisions (2017–2024)

in the DMA 2024 and had rules imposed upon it with proactive obligations, again signalling a shift from what was considered a breach and subsequently fined, to additional ex-ante regulation.

B. Amazon (Global, 2022–2025)

Amazon's self-preferencing practices or data misuse has been the subject of scrutiny across the world. In 2024, the Italian Competition Authority fined Amazon €1.2 billion in respect of self-preferencing its logistics, which further raised concerns - things we assume we know about the extent of a platform neutral stance.[72] In 2025, the ACCC's inquiry into Amazon's use of its marketplace raised concerns about coordination for platforms dealing with data related issues of dominance.

VI. Conclusion

The swift onset of algorithmic pricing and consumer profiling systems emerging in digital markets introduces an appealing combination of economic efficiency and personalization but also creates substantial risks to competitive integrity and consumer trust. Algorithms permit firms to identify and deploy offerings with unprecedented accuracy. Unfortunately, they can also intensify forms of implicit collusion and discrimination, often eroding market integrity. Whereas algorithms remove human discretion and exert control over pricing, we can observe the threat of supra-competitive pricing, diminished consumer welfare, and perhaps an avenue for regulatory scrutiny of these forms of collusion and market power through traditional anti-trust analysis.

In navigating this new environment, regulators, firms and policy-givers will need to work together in ordering the tradeoffs between innovation and ethics. We have pre-existing tools that can, in part, alleviate the likelihood of algorithmic collusion and exploitation by consumers, such as transparency, data sharing arrangements to share best practices, and dynamic regulatory mechanisms such as the EU's Digital Markets Act, while still upsides of innovation and technology. We can positively impact competition in consumer experience online marketplaces, as well as consumers' welfare anytime market outcomes are signal dependent on data driven decision making by working in the formats of decision-making and establishing precedents by linking competition and data authorities with educating consumers.

---

72 Italian Competition Authority, 'AGCM Fines Amazon €1.2 Billion' (2024); ACCC, Amazon Marketplace Inquiry Report (2025)