9th United Nations Conference on Competition and Consumer Protection
Room XIX, Palais des Nations
Geneva
7-11 July 2025

Enforcement Challenges in Addressing Algorithmic Collusion

Contribution

Mr. Daniel Favoretto

Competition Lawyer

This material has been reproduced in the language and form as it was provided. The views expressed are those of the author and do not necessarily reflect the views of UN Trade and Development.

9th United Nations Conference on Competition and Consumer Protection

Palais des Nations, Geneva, Switzerland

7-11 July 2025

Enforcement challenges in addressing algorithmic collusion

Contribution

Daniel Favoretto

Former UNDP Consultant

Competition Lawyer (EU-qualified)

Former NGA for the Brazilian Competition Authority (CADE) at the ICN

Guest Member of the UNCTAD Working Group on Cross-Border Cartels

Former researcher at the Research Centre of Competition, Public Policy, Innovation, and Technology (Comppit) of *Fundação Getúlio Vargas* (Brazil)

Summary

Preliminary note: This contribution represents only the author's position on a standalone basis, not necessarily the opinion of the institutions to which he is or has been associated with.

I. Introduction

Among the challenges brought by digital markets to competition law is the concern over algorithmic collusion, a topic that has been growingly approached by academic literature in the last years[1]. Like in every field, competition law enforcement must adapt to infringers' creativity and tactics to bypass deterrence. However, algorithmic collusion should not be oversimplified as a phenomenon of modern cartelists. As technology becomes endlessly intelligent, market players legitimately pursue new tools to dominate the markets in which they operate, increasing the risk of unintended algorithmic collusion in markets that have been largely far from the spotlight of anticartel enforcement.

This policy paper aims to map competition enforcers' challenges in addressing algorithmic collusion, by identifying the legal and practical bottlenecks for each stage of enforcement – *i.e.*, from early investigative techniques to compliance with remedies and sanctions. The ultimate question that this work aims to answer is: in view of balancing enforcement costs with due process of law, what are the challenges posed by algorithmic collusion to competition authorities?

While competition enforcers have received valuable guidance by the Organisation for Economic Co-operation and Development (OECD) on the topic of algorithmic collusion[2], this policy paper attempts to go a step further by providing a set of guiding questions to classify the collusion risk of an algorithm, besides presenting updated cases involving this topic.

A methodology to classify the collusion risk of an algorithm is crucial to enable a proportionate intervention by competition authorities. As collusion can become less based on human behaviour and more on artificial intelligence, proving an agreement under the standard of proof of collective infringements becomes harder (if not impossible), remaining either advocacy tools or unilateral conduct enforcement against algorithmic collusion. Algorithmic collusion is a phenomenon in which competition authorities still have little to no experience[3], but the rapid adoption of AI tools in the

---

[1] A landmark publication in this topic was Ezrachi's and Stucke's 2017 paper, which systematised the legal issues in potential collusive behaviour through artificial intelligence – Ariel Ezrachi and Maurice Stucke, 'Artificial intelligence and collusion: when computers inhibit competition' (2017), *University of Illinois Law Review*, v. 2017, n. 5, 1775-1809. Ever since, many scholars have highlighted tacit algorithmic collusion as a potentially growing threat to competition, e.g., Aneesa Mazumdar, 'Algorithmic collusion: reviving Section 5 of the FTC Act' (2022), *Columbia Law Review*, v. 122, 449-488.

[2] The earliest contribution by the OECD focused specifically on algorithmic collusion was the Roundtable on Algorithms and Collusion in the 127th meeting of the OECD Competition Committee on 23 June 2017. Available at <https://one.oecd.org/document/DAF/COMP/M(2017)1/ANN2/FINAL/en/pdf>

[3] This diagnosis is based on the contributions to the 140th OECD Competition Committee meeting in 2023. Available at <https://one.oecd.org/document/DAF/COMP/M(2023)1/ANN4/FINAL/en/pdf> Furthermore, "the magnitude of the threat from algorithmic collusion by autonomous self-learning algorithms is still disputed in the academic literature and there are few known cases" (OECD (2023), *Algorithmic Competition*, OECD Competition Policy Roundtable Background Note, p. 7

few known cases" (OECD (2023), *Algorithmic Competition*, OECD Competition Policy Roundtable Background Note, p. 7, www.oecd.org/daf/competition/algorithmic-competition-2023.pdf)

corporate environment demands these authorities to be ready to monitor and address the risks of this phenomenon.

This paper is structured in five sections, besides this introduction. Section II defines the phenomenon of algorithmic collusion and underlying concepts. Section III summarises the efficiencies and risks of business intelligence algorithms[4] for competition purposes. Section IV pinpoints known investigations of algorithmic collusion by competition authorities of UN member States, showing that the few existing precedents do not concern purely tacit (or machine-based) algorithmic collusion. Section V provides a step-by-step methodology for competition authorities to estimate the antitrust risk of business intelligence algorithms. Finally, section VI concludes by highlighting the potential challenges for each investigative technique that could be used to uncover the functioning of a business intelligence algorithm.

Given that this work is a contribution to a conference composed mostly of competition authorities and delegates representing nation-States, the approach adopted herein is pragmatic and unlimited to one jurisdiction. This short piece aims to be discussed among member States and serve as a useful source for competition authorities to balance the right approach against algorithmic collusion, avoiding both overenforcement and underenforcement.

II. What is algorithmic collusion?

Despite the basic nature of many of the concepts involved, a few clarifications are important, considering the lack of universal definitions in a subject widely debated. Firstly, algorithmic collusion means a collusion achieved through algorithms. An algorithm refers to a set of rules aimed at performing a task or solving a problem[5]. It has, therefore, a predefined set of commands and purposes. The concept is broad to the extent that it can easily be replaced by the concept of methodology (even a recipe to make a cake can be considered an algorithm[6]). However, for an algorithm to be relevant for competition law – at least considering the contexts in which it is usually debated –, it must be (i) digital and (ii) applied for business purposes. Algorithmic collusion is, therefore, a phenomenon of collusion between competitors through digital algorithms.

Secondly, algorithms are not the same as artificial intelligence (AI). While AI refers to the capacity of a machine to operate intelligently (including machine learning and deep learning as engineering attempts of artificially simulating human brain activity), algorithms can be based on these

[4] Whenever academic literature approaches the topic of algorithmic collusion, authors refer to pricing algorithms, as if algorithms are used only for pricing purposes. However, a market player's business strategy involves more than just pricing and, therefore, algorithms can be used for purposes beyond price. That's why this paper adopts a different nomenclature, *i.e.*, business intelligence algorithms rather than pricing algorithms.

[5] According to the Cambridge Dictionary, algorithm is "a set of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem". Britannica defines it as a "systematic procedure that produces—in a finite number of steps—the answer to a question or the solution of a problem". Respectively available at <https://dictionary.cambridge.org/dictionary/english/algorithm> and <https://www.britannica.com/science/algorithm>

[6] This wide concept was adopted in the BBC's Computing Science and Digital Literacy material, available at

- This wide concept was adopted in the BBC's Computing Science and Digital Literacy material, available at <https://www.bbc.co.uk/bitesize/articles/z3whpv4>

technologies to perform their functions[7]. These are the algorithms capable of generating tacit collusion with little to no human intervention.

Thirdly, algorithmic collusion does not necessarily refer to price-fixing collusion (and, therefore, pricing algorithms). As widely acknowledged by competition authorities and competition experts in recent years, due to antitrust cases in zero-price markets involving digital platforms, competition law is also concerned with other competition variables, such as quality and innovation. In whichever aspect of competition an algorithm plays a role, algorithmic collusion can take place, even if price is the usual focus of market players.

III. Efficiencies and risks of business intelligence algorithms

Addressing algorithmic collusion is not trivial for competition enforcers. The line between efficient technological tools for business decision-making and collusive tools to bypass competition can be tenuous. If authorities were to eliminate any risk of algorithmic collusion, it would be easier to simply ban business intelligence algorithms. However, besides potentially infringing constitutional principles of economic liberty and freedom of enterprise in many UN member States, such attempt would also kill important sources of efficiency to better serve consumers. In other words, that would amount to a typical situation of overenforcement.

Potential efficiencies of business intelligence algorithms include the ability to reflect cost variation and externalities into price, favouring allocative efficiency. In other words, if the decision to set the price is based on up-to-date data and objective criteria, the price of a product or service better represents its underlying costs and efficiencies, allowing for better-informed decisions in the market. Additionally, business intelligence algorithms can enable a more dynamic market, as market players can respond more quickly to competitors' strategies. In this sense, such algorithms can intensify competition.

However, due to its data processing capacity, algorithms can turn the market transparent and anticipate competitors' strategies, to the extent that parallelism between market players becomes the new tendency. In other words, the uncertainty about competitors' strategies fades away to the point where individual decision-making becomes less profitable than collective decision-making. In addition, this makes algorithms attractive tools for surveillance by cartelists wishing to enforce their anticompetitive agreements.

IV. UN members' experience with algorithmic collusion

Knowing similar cases in other jurisdictions is relevant for competition enforcers. It allows knowing who to contact in an international forum for formal cooperation or brainstorming purposes. It also gives a benchmarking example to reference in the national decision, enhancing legal reasoning

[7] OECD, 2023, p. 9 (*supra* note n. 3).

and proving that the position that the enforcer is taking is not unprecedented (thus, reducing his/her burden). Additionally, it may enable the mental anticipation of challenges, avoiding mistakes in an ongoing case. Bottom line: despite the singularities of each jurisdiction's legal framework, culture and market dynamics, experience shows that competition authorities commonly face similar enforcement challenges of at least some of their foreign counterparts.

A common question to United Nations' members that have approached this topic is whether current tools of competition law enforcement are sufficient to address algorithmic collusion. In other words, are legal provisions and enforcement practices enough to prohibit and deter this technological phenomenon?

In the United States, competition enforcers' perspective seems to be that, yes, current antitrust tools are sufficient to deal with these cases[8]. According to a joint brief submitted by the U.S. Department of Justice (DoJ) and the Federal Trade Commission (FTC) to a district court of Seattle on 03 January 2024, the case law applicable to anticompetitive conspiracies equally applies to the common use of a pricing algorithm by competitors, being sufficient for a per se illegality finding that competitors delegate the starting point of their prices to the same algorithms[9]. In other words, "price fixing by algorithm is still price fixing" [10]. This case was a class action brought against landlords who had agreed to use common pricing algorithms to set multifamily rents in the U.S.

Brazil seems to be in similar line, as exemplified by the Aprix case[11], concerning an alleged promotion of uniform commercial conduct by a business intelligence algorithm developer focused on the fuel retail sector. The preliminary proceeding was launched on 22 February 2021[12], based on online news of a Brazilian startup dedicated to the fuel sector, called Aprix. After replies by Aprix to the Brazilian Competition Authority's (CADE) requests for information and an analysis conducted by CADE's Department of Economic Studies, CADE launched an in-depth investigation on 19 November 2024[13].

While this case is ongoing at current date of writing and no negative judgement exists, CADE did not raise any question as to whether the current legal framework and the longstanding case law on collusive infringements were sufficient to frame the investigated conduct or to open an in-depth investigation[14]. Furthermore, this case shows the important involvement of economists (and data analysts, potentially) involved in investigations of algorithmic collusion.

[8] For the avoidance of doubt, in this work, antitrust and competition law are used as synonyms, despite the difference of scope that the concept of "antitrust" may have across the Atlantic.
[9] Case No. 2:23-cv-01391-RSL (Mckenna Duffy v. Yardi Systems, Inc. ***et al.***), joint brief available at <https://www.ftc.gov/system/files/ftc_gov/pdf/YardiSOI-filed%28withattachments%29_0.pdf>
[10] Open statement in the FTC blog, available at <https://www.ftc.gov/business-guidance/blog/2024/03/price-fixing-algorithm-still-price-fixing>
[11] CADE, Administrative Proceeding n. 08700.006280/2024-60.
[12] Order n. 04/2021, issued on 22 February 2021 by CADE's General-Superintendency.
[13] Order n. 23/2024, issued on 19 November 2024, based on Technical Statements n. 49/2024/CGAA8/SGA2/SG/CADE.
[14] This position is in line with CADE's contribution to the 140th OECD Competition Committee meeting in 2023 (*supra* note

[14] This position is in line with CADE's contribution to the 140th OECD Competition Committee meeting in 2023 (*supra* note n. 3), where CADE asserted "the Brazilian competition legislation to be more than sufficient to address and punish cases in

While useful precedents for benchmarking purposes, both cases described above still have potential "plus" factors that can facilitate their analysis. On the U.S. case, there was an agreement to use the algorithms by competitors. On the Brazilian case, the business intelligence algorithm was promoted by a sectoral association, along with public declarations that at least suggested an objective to harmonise business practices and avoid price reductions. In other words, the few existing precedents on algorithmic collusion are not purely tacit collusion cases, where parallelism resulted from artificial intelligence. Furthermore, the competition authorities, in both cases, did not adopt a methodology to classify the risk of the investigated algorithms from a unilateral perspective.

V. How to approach algorithmic collusion cases?

The first question that competition authorities have to ask themselves, when analysing the antitrust risk of a business intelligence algorithm, is: *(1) should this case be approached as a collective conduct or as a unilateral conduct?* The question seems trivial, but it is not. Although collusion assumes an arrangement between competitors (therefore, a collective conduct between different undertakings), technological development has reached a level where the use of certain product can promote uniform commercial conducts without the awareness of the market players that such uniform pattern is taking place. In other words, like allegedly in the Aprix case mentioned above, the uniform conduct can be a result of a third-party inducing the market players to operate accordingly[15].

Theoretically, the choice to open a unilateral conduct case or a collective conduct one depends on how the infringement was perpetrated. In other words, who caused the harm to competition: an undertaking individually or some undertakings jointly? In practice, however, the decision may be based on the applicable standard of proof and the evidence available. As widely adopted by competition laws worldwide, parallelism itself is not illegal (otherwise, the mere rational reaction to a competitor in an oligopolistic market could be considered illegal), so a competition authority must identify if a unilateral or collective behaviour is "pushing" the market towards such parallelism.

The second question to be addressed in a potential algorithmic collusion case is: *(2) how competitively sensitive are the algorithm's inputs?* The inputs of an algorithm determine the algorithm's capacity to predict the optimal market strategy for its clients. This means that the more competitively sensitive the inputs, the higher the potential of the algorithm reducing the market player's uncertainty about its competitors and, therefore, the higher the potential of collusion.

In other words, if the inputs of an algorithm include, for example, current prices practiced by competitors, costs, investments or list of customers per market player, the algorithm is more attractive

---

which the algorithm serves merely as a messenger tool", but that "it may prove exceedingly difficult (…) to establish the elements of intentionality and coordination (…) when there is no contact between players and any anticompetitive outcome may result from computational calculations that can choose price parallelism among other paths".

[15] This unilateral aspect is related to promoting an environment favourable to collusion, and should not be misunderstood with other forms of unilateral conduct perpetrated through algorithms, such as self-preferencing, predatory pricing, and

with other forms of unilateral conduct perpetrated through algorithms, such as self-preferencing, predatory pricing, and tying).

for market players, but also more likely to lead to collusion. This, of course, does not make the algorithm *per se* illegal or anticompetitive, since the factors below should be taken into account.

The third question worth asking when approaching a business intelligence algorithm is: *(3) does the algorithm refer to one specific/relevant market or is it a cross-market product?* In other words, what is the scope of the algorithm? The narrower the scope of the algorithm, the more limited is the field of competition to which the algorithms' outputs apply.

This means that, the narrower the scope of the algorithm (*e.g.*, limited to one relevant market), the narrower the pool of potential users, the more likely the outputs are to affect the targeted market, and the higher the risk of collusion. If the algorithm concerns many different markets, its outputs are less likely to reduce its users' uncertainty about their respective competitors.

Another question worth considering is: *(4) does the algorithm suggest a specific commercial conduct (e.g., price) or does it only provide data for its users to individually decide their strategies?* In other words, how imperative is the algorithm? As a matter of human behaviour, the more imperative the algorithm is, the higher its potential to influence market players' competitive strategies and, therefore, the higher the risk of causing collusion.

However, the line between being imperative and providing data can be tenuous. An algorithm may not explicitly suggest a certain market strategy (*e.g.*, price), but it may be so granular in the data provided as output that it largely influences its users' strategies, enabling a collusive environment[16].

A fifth question to be considered by enforcers is: *(5) how often does the algorithm provide outputs?* In other words, what is the recurrency of the algorithm's outputs? The higher the recurrency, the more likely it is that the algorithm's outputs accompany market dynamics and, therefore, dictates the competitive strategy of its users. For example, an algorithm that provides outputs on a daily basis (or in a shorter timeframe) is more likely to enable collusion than an algorithm that issues outputs on a monthly basis.

However, competition authorities should avoid sticking to absolute assumptions or magic numbers. The analysis must be made on a case-by-case basis, according to the dynamics of the market at hand. The fact that an algorithm issues outputs on a monthly basis, for example, does not necessarily rule out the possibility of it causing collusion, in case market players decide on a given competitively relevant factor once per month.

A sixth question that is important to come to enforcers' mind is: *(6) does the algorithm enable oversight of competitors by its users?* The more an algorithm can be used to monitor competitors, the more it can serve as a tool for collusive behaviour. This could occur if the algorithm produces updated

[16] A similar remark was raised in the U.S., by the FTC (2024), when analysing the rental algorithms case: "an agreement to use shared pricing recommendations, lists, calculations, or algorithms can still be unlawful even where co-conspirators retain some pricing discretion or cheat on the agreement". Available at <https://www.ftc.gov/business>

some pricing discretion or cheat on the agreement". Available at <https://www.ftc.gov/business-guidance/blog/2024/03/price-fixing-algorithm-still-price-fixing>

data to a granular extent that it enables the user to monitor the market strategies of individual competitors.

However, two disclaimers are important. Firstly, the fact that an algorithm does not enable monitoring of competitors does not necessarily prevent it from causing algorithmic collusion, given that, for such type of collusion, market players do not necessarily have to be actively engaging into a cartel (*i.e.*, users individually following an algorithm that provides uniform outputs can constitute a collusive environment), as explained in section III above. Secondly, the possibility of an algorithm serving as a monitoring tool also depends on the market structure in which it is used (algorithmic outputs about the market as a whole in highly oligopolistic markets may allow monitoring).

VI. What challenges arise for each investigative technique?

To conclude, it is worth identifying the challenges faced by competition enforcers according to the investigative technique used to tackle algorithmic collusion. Although the challenges may vary per jurisdiction, such as the precise legal provisions governing the investigative body's mandate and its limits, some common challenges tend to come up across jurisdictions.

The first form of investigation is issuing requests for information (RFIs) to market players, including the investigated party. While straightforward, this form of investigation suffers from two sensibilities, namely, by disclosing the fact that an investigation is being conducted and by relying on the notified party's willingness to contribute to the investigation. Although RFIs in antitrust investigations usually bear the condition of mandatory reply, subject to coercive sanctions and statements of oath, it gives very limited visibility of internal corporate information to competition authorities.

A real-life perspective shows that, to address competition authorities' RFIs, market players go through a process in which the internal data goes from the business departments to the in-house legal team, then to the external lawyers, and finally to the competition authorities. In a chain involving people with different positions, data can be overseen, misinterpreted or omitted, on purpose or unintendedly. This could especially be the case in algorithmic collusion, where the investigation may involve understanding how the algorithms work, something that is commonly treated as highly confidential and technical.

Another form of investigation is dawn raids, also known as search-and-seizure operations in some jurisdictions. This is perhaps the strongest form of intervention by a public authority, and it surely enables access to privileged evidence. However, due to their level of intervention in private premises, depending on the jurisdiction's legal framework, dawn raids must be used proportionally and limited to facts subject to criminal prosecution, such as hardcore cartels. Additionally, practice shows that dawn raids demand significant organisational effort by the competition authority; from obtaining the

necessary court order on a confidential basis to coordinating the inspection visit with different teams and in different locations.

Furthermore, the location (within a corporate structure) of the evidence necessary to open or close an algorithmic collusion case may not always be clear. The people entitled to access to information about how a certain algorithm works can be very limited. This is why dawn raids tend to be more effective for cases of hardcore cartels where algorithms are used as a tool for a broader anticompetitive agreement (*i.e,*, when the collusion is human-originated rather than machine-originated). For such cases, references to anticompetitive use of algorithms can be widespread within a corporate structure and, therefore, easier to spot in a search-and-seizure inspection.

Besides the more traditional investigative techniques mentioned above, a particularly relevant one for algorithmic collusion is algorithmic auditing[17]. Competition authorities have been strengthening their staffs with new roles, such as data analysts, to enable these modern forms of investigation. Algorithmic auditing can take place through many methods, each of which have their own limitations and challenges.

For example, scraping audit consists of writing a code to automatically collect the desired data in an online webpage or platform. While this technique does not require cooperation from the investigated party, it requires the development of a code customised to the investigated algorithms and can malfunction or underperform if the algorithms suffer any minor change or update by the investigated party[18]. Reverse-engineering is another effective investigative method, but, depending on whether the competition authority has access to the source code or to an authentic copy of it, the process may rely heavily on inferences and, therefore, not meet the required standard of proof.

To conclude, it is crucial to have in mind that the challenges to all of the investigative techniques mentioned above equally apply to the monitoring of compliance to remedies, in case the collusion risk of a business intelligence algorithm has been addressed through structural or behavioural remedies targeted at the functioning of the algorithms.

This challenge is even greater if the remedies were agreed in a settlement between the investigated party and the competition authority. As highlighted in academic literature, designing the right antitrust remedies through a settlement involves the challenge of balancing between negotiation costs and enforcement costs (the more targeted the remedy, the higher the negotiation costs and the lower the enforcement costs; the broader the remedy, the lower the negotiation costs and the higher the enforcement costs).

---

[17] "[A]n algorithm audit is a method of repeatedly and systematically querying an algorithm with inputs and observing the corresponding outputs in order to draw inferences about its opaque inner workings" Danaë Metaxa, Joon Sung Park, Ronald E. Robertson, Karrie Karahalios, Christo Wilson, Jeff Hancock and Christian Sandvig (2021), "Auditing Algorithms", *Foundations and Trends in Human-Computer Interaction*: v. 14, n. 4, 288

Foundations and Trends in Human-Computer Interaction. v. 14, n. 4, 288.
[18] OECD, 2023, p. 29 (***supra*** note n. 3).

This challenge of balance is sensitive in cases of algorithmic collusion, because, despite a risk of collusion that may be present, business intelligence algorithms are innovation-intensive products, so competition authorities are put in the delicate position between risking underenforcement (*i.e.*, not addressing sufficiently the collusion risk) and overenforcement (*i.e.*, undermining incentives for innovation and investments)[19].

[19] Daniel Favaretto, 'Enforcement antitruste em mercados digitais: o CADE e os remédios em fusões nos mercados de

[11] Daniel Favoretto, 'Enforcement antitruste em mercados digitais: o CADE e os remédios em fusões nos mercados de inovação' (2020), ***Defesa da concorrência em plataformas digitais*** (Caio Mario Pereira Neto), FGV, 312-335.