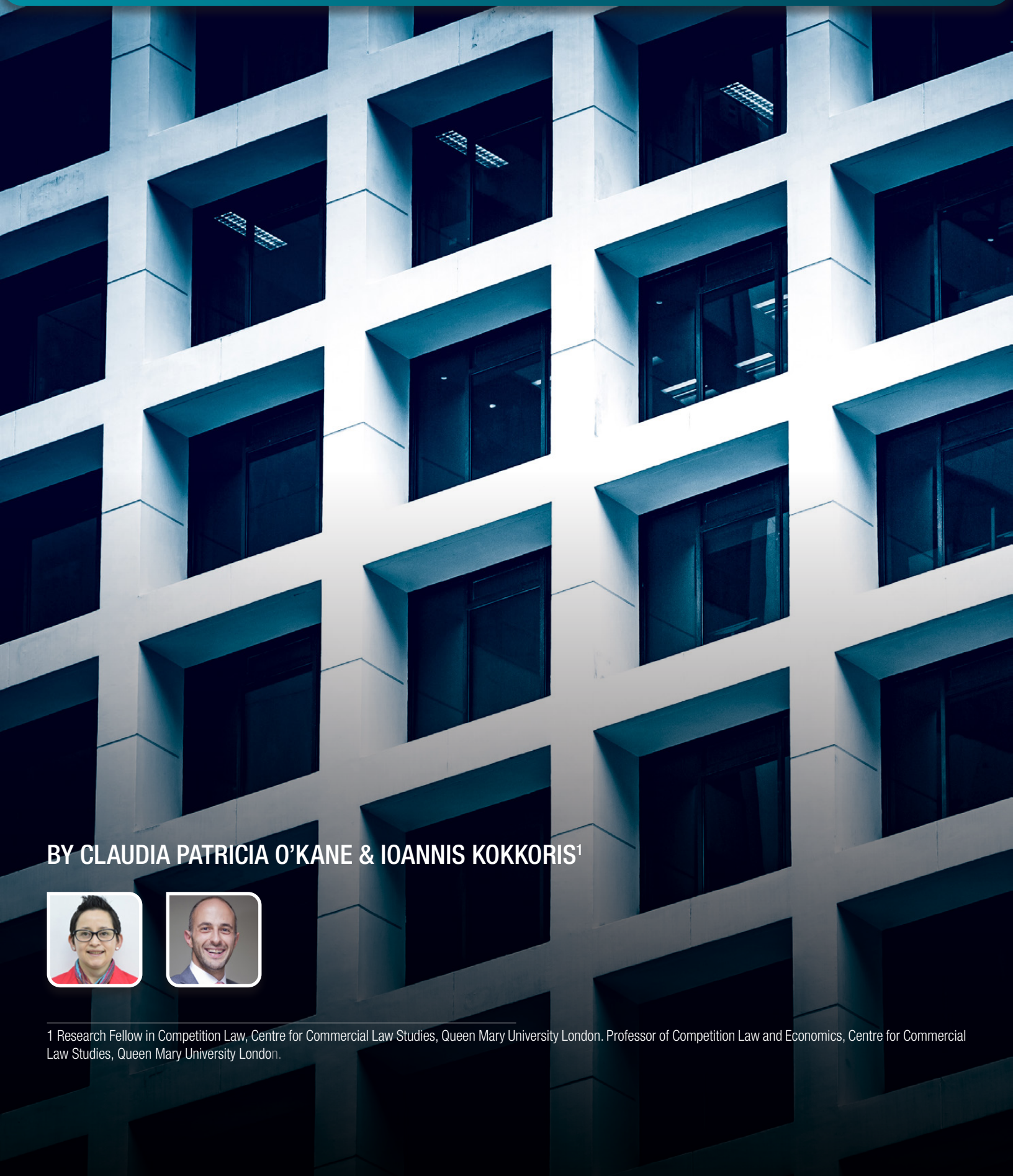
A FEW REFLECTIONS ON THE RECENT CASE LAW ON ALGORITHMIC COLLUSION



BY CLAUDIA PATRICIA O'KANE & IOANNIS KOKKORIS[1]

1 Research Fellow in Competition Law, Centre for Commercial Law Studies, Queen Mary University London. Professor of Competition Law and Economics, Centre for Commercial Law Studies, Queen Mary University London.

CPI Antitrust Chronicle July 2020

www.competitionpolicyinternational.com

I. INTRODUCTION

Technology and its rapid development while transforming businesses is testing the boundaries of the current approach to competition enforcement and practice. Such challenges have shifted the attention of competition authorities, scholars and governments, and are now the main topic of a large number of papers, seminars and discussions. Yet, even if the debate is stimulating, two shortfalls appear evident: (i) the limited understanding of the technologies and their implications, particularly amid certain stakeholders, and (ii) the scarcity of extensive evidence confirming the veracity of the prevailing theories.

One of the most recent challenges in competition enforcement is that of algorithmic collusion. Concerns have been voiced that unless competition authorities improve their investigative tools, it is unlikely that they will be able to deter the use of algorithms in contributing or instigating collusive conduct.[2]

This paper begins by providing a definition of what an algorithm is, a brief description of three identified scenarios where collusion may emerge as a result of the use of algorithms, and an assessment of some prominent characteristics of the limited number of cases where the use of algorithms was found to be a factor that was contributing to collusion. The paper aims at identifying some key lessons that can be drawn from the literature and precedents. The paper also raises the question whether by making software providers liable deterrence could be created in the use of algorithms for collusion.

II. ALGORITHMS AND COLLUSION

A simple and common definition of an algorithm is *"a computable set of steps to achieve a desired result."*[3] There are a variety of more elaborate definitions, but for the purposes of our analysis we define an algorithm as: *"a finite, abstract, effective, compound control structure, imperatively given, accomplishing a given purpose under given provisions."*[4]

It has been argued that algorithms can be used for price setting or for repricing strategies.[5] Literature has identified the following three scenarios where algorithms could enable an anticompetitive conduct: (1) there is a previous agreement between competitors and the algorithm is used

2 Schrepel, Thibault, "Collusion by Blockchain and Smart Contracts," *Harvard Journal of Law & Technology* 33 (2019):160.

3 Subburaj, Ramasamy, "Programming in C," *Vikas Publishing House PVT LTD* (2nd edn, 2014): 5.

4 Hill, Robin K., "What an Algorithm Is," *Philos. Technol.* 29 (2016): 35–59, https://doi.org/10.1007/s13347-014-0184-5.

5 Autorite de la Concurrence and Budeskartellamt, "Algorithms and Competition," at 5, November 2019; available at https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_WorkingPaper.pdf;jsessionid=847C7C9FE98C-4CC03C4C66E5CFCE13BB.2_cid371?__blob=publicationFile&v=5.

as a vehicle to implement it; (2) there is no direct communication between competitors but an alliance is derived through a third party algorithm, and (3) the alignment results from the plain interaction and adaptation of the algorithms.[6]

In relation to the first scenario, the algorithms could be used to monitor the competitor's price determinations, to identify possible deviations and to react to these deviations (known as monitoring algorithms),[7] or they could automatically adapt the prices of the cartelists to market changes (known as parallel algorithms).[8] In the second scenario, in the absence of communication among the members of the cartel, the use of a third party signaling algorithm can lead to the alignment of their actions.[9]

In the third scenario, self-learning algorithms that have been initially designed to enhance profits, independently (without human intervention) could recognize and implement tacit collusion as an effective method to achieve such a goal.[10] This relates to the "machine learning" capacity of an algorithm, whereby through a multitude of pricing permutations, the algorithm will "inadvertently" lead to price collusion as a means to achieve its aim which is to maximize profits for the companies.[11] These types of algorithms and the ensuing price collusion is the most controversial from a competition enforcement perspective, as it may not always be possible for the competition authority to prove the "meeting of minds" or "concurrency of will" of the cartelists.[12]

Against this theoretical framework, the purpose of the next section is to review some of the first cases we have on algorithmic collusion, with the aim to identify the challenges that competition authorities face in this area of enforcement.

III. CASE LAW ANALYSIS

A. Posters and Frames Case in the UK

In 2016, the CMA decided that Trod Limited ("Trod") and GB eye Limited ("GBE") had infringed the prohibition contained in section 2(1) of the Competition Act 1998 by agreeing that *"where there was no cheaper third party seller on the online retail platform www.amazon.co.uk ('Amazon UK'), they would not undercut each other on prices."*[13] The parties sold licensed sport and entertainment merchandise and related products, where GBE was a supplier of Trod, and both were competitors on the Amazon marketplace. After several complaints from Trod about the low prices offered by GBE on the online platform, GBE, aiming to maintain good relations with Trod as its customer, agreed not to compete with it in the online market. At the beginning, the parties tried to manually implement the agreement, but given the difficulties in monitoring, collecting and adjusting the prices, they decided to use a repricing software.[14]

6 *Id.* at 2-4.

7 Background Note by the Secretariat, "Algorithms and Collusion," OECD Doc. DAF/COMP(2017)4, at 24,25 (June 9, 2017); available at https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf [https://perma.cc/29VF-2RFT].

8 *Id.* at 26–27.

9 *Id.* at 28-29.

10 Ezrachi, Ariel & Stucke Maurice E., "Sustainable and Unchallenged Algorithmic Tacit Collusion," *NW. J. Tech. & Intell. Prop.* 17, 217 (2020): 250-251. https://scholarlycommons.law.northwestern.edu/njtip/vol17/iss2/2; Background Note by the Secretariat, *supra* note 7, at 30-31.

11 Ezrachi, Ariel & Stucke Maurice E., "Artificial Intelligence & Collusion: When Computers Inhibit Competition," (April 8, 2015) *University of Illinois Law Review* 5, 1775-1809 (2017): 1795. Michal Gal describes this process as the capacity that the algorithm has to *"teach itself the best way to behave in the market even if the coder did not model such conduct,"* see Gal, Michal, "Algorithmic-facilitated coordination: market and legal solutions," *CPI Antitrust Chronicle* May (2017): 28.

12 Schwalbe, Ulrich, "Algorithms, Machine Learning, and Collusion," *Journal of Competition Law & Economics* 14(4), 568-607 (2019): 597; Deng, Ai, "When Machines Learn to Collude: Lessons from a Recent Research Study on Artificial Intelligence," 6, available at https://ssrn.com/abstract=3029662.

13 Trod and GBE, case 50223.

14 *Id.*

Thus, each party acquired a separate piece of automated repricing software. GBE's software was programmed to match Trod's price in the event that there was no cheaper third-party seller on Amazon. Meanwhile, Trod's software was designed to use the "ignore function"[15], signifying that GBE was excluded from the regular rules that Trod had arranged through its software for undermining competitors. After examining all of the collected evidence, the CMA concluded that the repricing software assisted the parties not to undermine each other's prices and to inhibit competition between them.[16]

There are a number of interesting implications arising from this case. The conduct of Trod and GBE provides a clear illustration of how the use of monitoring and parallel[17] algorithms facilitated the implementation of a prior agreement. As they could not otherwise effectuate their collusive agreement the companies resorted to an algorithm to achieve their aim; the evidence the CMA presented include parties' statements that, *"Logistically it is going to be difficult to follow the pricing effectively on a daily basis so I am looking into re-pricing software…."*[18]

What is also relevant in this case is the amount of interaction between the parties via email in order to adjust the functioning of the software, an element which undoubtedly backed the findings of the authority. Without such evidence the outcome of the investigation could have been different, implying that detecting algorithmic collusion is not as straightforward as collusion based on hard evidence. But, at the same time this reveals that, at least in this case, the human interaction once the algorithm was in place was still an element of the implementation of the agreement, which illustrates the challenges of substantiating algorithmic collision in the absence of communication between the companies.[19] Another important aspect is that the investigation started after GBE's application for leniency, which on the one hand supports the effectiveness of the leniency program, but on the other casts doubt on whether the anticompetitive conduct would have been discovered without GBE's leniency application.

B. Electronic Goods Manufacturers Case in the EU

In 2018, the European Commission fined the electronic goods manufacturers Asus, Denon & Marantz, Philips, and Pioneer for restricting online retailers to determine their resale prices independently and pressuring them to maintain higher prices for electronic products such as kitchen appliances, notebooks and hi-fi products.[20] The four manufacturers targeted their online retailers who offered their products at low prices by intimidating them and threatening them with sanctions, such as blocking supplies and bonuses, if they did not comply with the requested price level. Compliance was facilitated by the use of algorithms that monitored the resale price setting in the supply and adjusted prices to those of competitors when price decreases occurred.[21]

A first relevant aspect in this case is that the headquarters of the four infringers were based in different parts of the world, that is Asus in Taiwan, Denon & Marantz in Japan, Philips in the Netherlands, and Pioneer in Japan, whose actions affected consumers in France, Germany, the Netherlands, and other Member States, which shows the wide impact that such a type of coordination improved by the use of algorithms can have.[22] Thus, we could expect a larger number of global cartels being implemented easier now with the use of algorithms. A second aspect that deserves attention is that the EC reported that the implementation of the business strategy was confirmed by a number of documents, particularly

15 The software allowed Trod to design 'repricing profiles' (known as the 'compete rules'), so the software modified Trod's prices automatically in response to the prices of competitor's products, but by adding GBE to the "ignore function" the 'compete rules' of the software did not apply to its co-cartelist. See Trod and GBE, case 50223, *supra* note 13, at para 3.81.

16 Trod and GBE, *supra* note 13.

17 Parallel algorithms could be programmed to automatically retaliate discounts offered by other businesses and/or to emulate competitor's price changes in real time. See Capobianco, Antonio & Gonzaga Pedro, "Algorithms and Competition: Friends or Foes?," *CPI Antitrust Chronicle August* (2017): 3.

18 Trod and GBE, *supra* note 13, at para 3.57.

19 Ezrachi & Stucke, *supra* note 10, at 230; See also Schwalbe, *supra* note 12, at 570.

20 Press release: European Commission, Antitrust: Commission fines consumer electronics manufacturers for fixing online resale prices, (24 July 2018); available at https://search.yahoo.com/search?ei=utf-8&fr=aaplw&p=Press+Release:+EU+Commission,+Antitrust:+Commission+fines+Four+Consumer+Electronics+Manufacturers+For+Fixing+Online+Resale+Price+(24+July+2018).

21 Bentley, Philip, Buhart Jacques & Muto Mai, "The EU Commission fines electronic good manufacturers for resale price maintenance, (Asus/Denon & Marantz/Philips/Pioneer)," 24 July 2018, *e-Competitions* July 2018, Art. No. 89749; available at https://www.concurrences.com/en/bulletin/news-issues/july-2018-en/the-eu-commission-fines-electronic-goods-manufacturers-for-resale-price.

22 *Id.*

the written communications that the manufacturers sent to the retailers informing them about the policy and afterwards warning them about the consequences of not observing it,[23] a factor that seems to attest that communication is necessary to sustain the conduct. Similarly, it shows that given the type of physical evidence available the findings of algorithmic collusion were easily supported.

It is also noteworthy that the investigation started with unannounced inspections,[24] showing a proactive approach from the EU following its findings of its e-commerce enquiry published in May 2017, which indicated the *"increased use of automatic software applied by retailers for price monitoring and price setting"* to impose resale-price restrictions.[25] Such an approach is particularly welcome especially in the current conditions where the pandemic has increased e-commerce transactions by 74 percent compared to the same period last year[26] and it seems that this trend will remain.

C. Posters Case in the U.S.

On April 6, 2015, the DOJ announced the first criminal prosecution in e-commerce, where an agreement to fix the prices of popular posters that were traded on Amazon was facilitated by the use of algorithms that harmonized price changes among the co-cartelists and matched them accordingly.[27] The DOJ explained that the conspirators had instructed their algorithm to look for the lowest price proposed by a "non-conspiring" competitor, and then set their prices just under, which allowed their products to be close to the *"top of the search query without having to compete with each other."*[28] In the press release, the DOJ indicated that this case emerged as a result of a continuing federal antitrust investigation into price fixing in the online wall décor industry, which reflects the emphatic commitment to *"investigate and prosecute individuals and organizations seeking to victimize online consumers."*[29]

A vital insight from this case is the focus of the DOJ on discovering and enforcing collusive action in e-commerce, which parallels the same interest shown by the EC. The use of market studies appears to be a useful tool to identify market conditions that can enhance anticompetitive conducts, considering that the electronic goods manufacturers case in the EU as well as this case emerged after the authorities had conducted market studies in the e-commerce sectors. The case also shows that once again the automated software did not limit its functioning to just monitoring prices but also led to their coordination, which clearly simplified the implementation of the agreement and was an important factor in the appointment of liability for the collusive conduct.

23 Case AT.40465 – ASUS para 30 – 33.

24 *Id.* at para 15-16.

25 Press release: European Commission, *supra* note 20. See also Kalintrini, Andriani & Stones Ryan, "FIDE Congress 2020 – EU Competition Law and the Digital Economy: United Kingdom Report," *City Law School Research Paper 2019/06* (October 13, 2019): 2-3, available at https://openaccess.city.ac.uk/id/eprint/23431/1/Kalintiri%20and%20Stones%20%20CLS%20WP%202019-06.pdf, where CMA found that algorithms were used to monitor compliance with business policies (RPM) in the following online cases: Digital pianos and digital keyboards, light fittings, commercial refrigeration, bathroom fittings, and mobility aids – Pride.

26 Coker, James, "Covid-19: Huge growth in eCommerce sales during March," (April 7, 2020); available at https://www.essentialretail.com/news/growth-ecommerce-sales-march/.

27 Justice News, "Department of Justice: Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Martketplace Prosecution," (April 6, 2015); available at https://www.justice.gov/opa/pr/former-e-commerce-executive-charged-price-fixing-antitrustdivisionsfirstonline-marketplace.

28 Egerton, John, "DOJ Charges Poster Peddlers with Algorithmic Collusion on Amazon Marketplace," (Multichannel News, Nov 7, 2018); available at https://www.multichannel.com/news/doj-charges-poster-peddlers-with-algorithmic-collusion-on-amazon.

29 Justice News, Department of Justice, *supra* note 27.

IV. A FEW BRIEF REFLECTIONS

Although it has been recognized that optimization software seeks to prevent price wars,[30] which in itself could constitute an anticompetitive conduct, the existence of additional functions, different from just collecting data, that once integrated into the algorithm permits the consolidation of a tacit agreement could be enough to challenge the anticompetitive conduct, relieving the authorities from the duty of providing evidence of communication among the cartelists.[31]

In our opinion, software developers can be liable for willingly and knowingly designing an algorithm that can implement collusion (we refer here at scenarios one and two). This possibility for liability can limit the software scope to functions that will not induce collusion.[32] Hence, software developers would be more inclined to ensure that their algorithms do not breach competition law.

Equally, companies have an important responsibility in the lawful use of pricing software and cannot excuse their anticompetitive conducts by simply allocating the responsibility to the algorithm. In addition, they can be asked to ensure intra-company awareness and a culture of compliance by, for instance, tailoring constructive compliance schemes where the involvement of the IT department in its development is critical, as they are key members in the development of algorithms. For this reason, they need to be aware of the importance of complying, of the consequences of violating antitrust laws through the wrong use of algorithms, and of the need of assisting the company in identifying software abnormalities.

Thus, when a company is signing a supply contract with a developer of a price algorithm program, a copy of the compliance scheme should be given as part of the documents of the contract, and it should be signed by the representatives of the IT department of the buyer. Additionally, the company needs to regularly disseminate the compliance scheme among the members of the staff – and the attendance of the members of the IT department must be compulsory and recorded.

Additionally, in light of the second scenario where the 'hub' (the provider) aligns the action of the 'spokes' (the companies) through the use of a pricing algorithm, it is necessary to examine the extent to which sensitive information needs to be transferred to the software provider and how to protect it from being misused.[33]

V. CONCLUSIONS

The previous case law analysis leads us to draw the following conclusions. First, it is evident that enforcement took place in the first scenario where monitoring and parallel algorithms were key in the implementation of prior collusive agreements. At this point we do not seem to have cases referring to scenarios two and three, which can be an indication of the challenge's competition authorities face in bringing such cases. Similarly, having observed that the use of special codes or programming instructions beyond monitoring the prices enabled the implementation of a collusive agreement, we advocate the introduction of boundaries in the design of these types of software, being thus in agreement with Ezrachi and Stucke who have argued for the integration of *"ethics and legality into a computer program"*[34] or as EU Commissioner Vestager put it *"compliance by design."*[35]

The analysis of the cases has also revealed that the enforcement was supported by significant documented evidence. Enforcement may not be so straightforward when evidence of communication between the parties is absent. In such a case, the adoption of the compliance by design approach would lead to liability for the developers of the algorithms who knowingly created algorithms that could contribute or instigate collusion. This policy would also assist enforcement in the second scenario, where it would be enough for the authority to demonstrate that the market players had the same software provider, and they used identical algorithms that facilitated the collusive practice. In these circumstances,

30 Sathe, Abhijeet, "How Retailers and Brands Can Avoid the Race to the Bottom in Online Pricing, INTERNET RETAILER," (July 9, 2018); available at https://www.digitalcommerce360.com/2018/07/09/how-retailers- and-brands-can-avoid-the-race-to-the-bottom-in-online-pricing/ [https://perma.cc/3YDF-EZXY].

31 Ezrachi & Stucke, *supra* note 10, at 221.

32 Perhaps sanctions such as impeding their use for a period of time would work as an effective deterrent mechanism.

33 *Supra* note 5, at 37.

34 Ezrachi & Stucke, *supra* note 10, at 225.

35 Background Note by the Secretariat, *supra* note 7, at 46.

users would have the burden of demonstrating the lack of common understanding and the provider of the software would need to illustrate the lack of negligence.

Thus, contrary to the situation observed in the bricks-and-mortar economy, where monitoring, matching prices, absent any evidence of communication between the parties, is unlikely to lead to an infringement decision, in the online sector, if a firm provides identical algorithmic software to different competitors who have a common understanding (the common understanding derives from the use of parallel algorithms or functions such as the "ignore list") but there is no communication between them, as stated by the U.S. agencies such a situation *"would not be a bar to finding an unlawful conspiracy."*[36] Such an approach would prevent cases like the U.S. airline industry investigation during the 1990s, where a third party using sophisticated algorithms coordinated tariffs among the members of the cartel but explicit coordination was difficult to prove, from remaining unchallenged.[37]

Also, seeing that the posters cases in the UK and the U.S. took place through Amazon, perhaps policy makers would also benefit from exploring whether those market platforms could contribute by creating some rules with the aim of preventing or detecting the use of algorithms that distort online competition. Another interesting development is the increased proactiveness shown by the EU, the U.S., and the UK in detecting wrongdoing in the online sector by launching market studies and launching investigations, a trend that has been also observed in Australia, Brazil, China, Japan, Singapore, and other countries, which have recognized the online sector as part of their enforcement priorities,[38] something that is ever more important with the e-commerce growing significantly in the wake of COVID-19.

In relation to the third scenario we discussed above, we consider liability of the user or the provider to be challenging for competition authorities, as machine self-learning goes beyond human control and lacks a fundamental element in this type of conduct, which is the agreement or the common understanding or meeting of minds between competitors.

The cautious and balanced adoption of a new enforcement approach orientated to lessening the type of evidence that at the moment is required to challenge collusion using algorithms, particularly when communication is absent, is necessary to increase enforcement in this area. Equally, agencies need to develop new tools to understand this type of software, and perhaps explore cooperation with the digital platforms with the aim of identifying and preventing the use of collusive algorithms.

Even if there has been an increase in focus on the detection of competition restraints in online markets, the number of investigations remains low, signaling that stronger enforcement is required by competition authorities; and perhaps more e-commerce market studies, which have been proved to be effective, should be conducted. Finally, this paper seems to reject the claim that the use of algorithms at this point in time and with the current development in enforcement, relinquishes the need for communication between the members of the cartel, as the case law analysis showed communication was required to substantiate the anticompetitive conduct.

36 Directorate for Financial and Enterprise Affairs, Competition Committee, "Algorithms and Collusion – Note by the United States," OECD Doc. DAF/COMP/WD(2017)41, at 6 (May 26, 2017); available at https://one.oecd.org/document/DAF/COMP/WD(2017)41/en/pdf.

37 Background Note by the Secretariat, *supra* note 7, at 29.

38 Linklaters, Global cartel enforcement in 2018; available at https://www.linklaters.com/en/insights/publications/2018/april/global-cartel-enforcement-in-2018.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.