Artificial Intelligence and Antitrust: When Do Algorithms Violate Competition Laws?

I. What's the issue?

In the U.S., European Union, United Kingdom, and nearly every other jurisdiction with a competition law regime, it is *per se* illegal for competitors to fix prices or output, rig bids, or allocate markets or customers between themselves. Where agreements or information exchanges between competitors do not fit obviously into these categories, they may nevertheless be found illegal if they unreasonably restrain competition. In the U.S., under the "rule of reason" analysis, a restraint's anticompetitive effects are weighed against its non-pretextual, procompetitive benefits or justifications. Other jurisdictions apply similar weighing approaches to non-*per* se illegal agreements.

All of these inquiries are highly fact-intensive, and they often require the targets of the inquiry to engage in costly investigations or litigation. As such, companies are well-advised to try to avoid even the appearance of impropriety, or else face substantial costs fending off questions, demands, and even lawsuits from regulatory authorities, as well as individual or class action lawsuits.

The modern versions of competition laws first came into being toward the end of the 19th century and they have struggled at times to keep up with technological progress and the nuanced ways competitors could conspire or otherwise restrain competition. The core requirement for concerted action claims has always been that there is an actual agreement between competitors. However, technology can facilitate "tacit collusion" – where competitors in a concentrated market do not explicitly agree to act in concert, but nevertheless parallel one other on price or other competitive metrics – that does not necessarily rise to the level of illegal collusion, but nevertheless has the same anticompetitive effects an explicit cartel would cause.

Artificial intelligence ("AI") presents a novel application of these principles. When machines can make independent decisions, serious questions arise regarding whether competitors explicitly or tacitly agree to conspire or whether their AI simply acts in a way that is reactive to market conditions, which may include acting in parallel to a competitor. Indeed, it is entirely possible that two or more competitors' respective AIs might essentially begin to collude on price or other matters, but the actual human decision makers at the companies are completely unaware of that collusion (or, to paraphrase terminology from the antitrust laws, engage in "*un*conscious parallelism"). This in turn raises the question of whether companies can be liable under competition laws if non-human actors coordinate pricing or other competitive activities.

The very short answer—at least, as of this memorandum's publication—is "it depends." The longer answer is that competition laws seem well-suited to address certain types of AI-related collusion, but ill-suited under current statutory frameworks to address other types of parallel conduct. Regarding the former, recent investigations, as well as the core principles underlying competition laws, suggest that algorithmic cartels will be treated in the same way as traditional cartels. Tacit collusion arising from AIs' independent actions, however, seems not actionable under current competition laws, *if* it arises naturally from an AI's own decision making and adaptations, rather than core principles coded into an AI that are meant to encourage and facilitate coordination with competitors.

II. What is an algorithmic cartel and why would it be treated like other cartels under current antitrust laws?

An algorithmic cartel is probably the easiest type of AI-related conspiracy to assess. That type of coordinate activity is one in which competitors agree to use their respective AIs to collude, whether on price, product output, or other means, such as rigging bids or staying out of each other's way in various geographic markets or for certain customers. In these instances, the core behavior—agreeing with competitors to restrain competition in obviously illegal ways—remains the same; it is just the tools used to effectuate the illegal agreement that are different. Thus, illegality under existing competition laws seems similarly clear.

An example of this in practice is the U.S. Department of Justice's successful prosecution in *U.S. v. Topkins*, No. 15-00201 (N.D. Cal. 2015). There, Topkins and other e-commerce art sellers used pricing algorithms as a tool to eliminate any online price differences among themselves. The conspirators agreed to set prices in a certain way and then wrote pricing algorithms to effectuate that agreement. In its prosecution, the DOJ sought convictions for *per se* price fixing, because the competitors' AI just represented the means by which they effectuated their unlawful agreements to fix prices.

Similarly, in a related matter, the UK's Competition and Markets Authority issued a decision on August 12, 2016 finding that Trod Limited and GB eye Limited (trading as "GB Posters" in the UK) violated competition laws by agreeing that they would not undercut each other's prices for posters and frames sold on Amazon's UK website in certain circumstances. The parties ensured compliance with this agreement by using an automated repricing algorithm that monitored and adjusted their respective prices to ensure that neither was undercutting the other. The parties also kept in contact with each other through regular means to ensure the arrangement was working, and to deal with issues regarding the operation of the re-pricing algorithms.

III. Can I be liable if my AI pricing algorithm starts to collude with other AI algorithms?

In the U.S., legal scholars have grappled with the situations in which tacit collusion can and cannot give rise to liability. One famous example is Judge Richard Posner, who made a very public about face on this issue. In 1969, Judge Posner wrote an article, *Oligopoly and the Antitrust Laws: A Suggested Approach*, 21 Stan. L. Rev. (1969), which argued that evidence of tacit collusion and conscious parallelism between competitors should be illegal under Section 1 of the Sherman Act. Over 40 years later, however, as a Judge on the Seventh Circuit Court of Appeals, Judge Posner wrote an opinion in *In re Text Messaging Antitrust Litigation*, 782 F.3d 867 (7th Cir. 2015), that took the exact opposite view. In that opinion, which dismissed the case, Judge Posner explained that, although there was strong evidence that the defendant competitors followed one another on certain types of text messaging fees, doing so was self-evidently rational economic conduct and not the result of any explicit agreements. He also noted that making tacit collusion illegal created more problems than it solved, since competitors likely could not accurately predict what sort of independent pricing decisions were and were not illegal. He therefore dismissed the case for not stating a claim under Section 1 of the Sherman Act.

The difficult question that arises in light of this law is whether companies can be liable when their AI independently concludes that colluding with competitors will maximize revenues or profits. Such "algorithmic tacit collusion" has not yet been tested in court, but it is a real problem for

competition, because AIs have already realized that colluding even tacitly with competitors can be very profitable.

For example, the United Kingdom's competition regulatory agency, Competition & Markets Authority ("CMA"), published a study in October 2018 regarding pricing algorithms and how they affect competition. The study found "evidence of widespread use of algorithms to set prices particularly on online platforms," and that, based on "simple pricing rules provided by the platforms themselves, some third-party firms sell more sophisticated pricing algorithms to retailers or directly take on the role of pricing using computer models on behalf of their clients."[1] The problems for competition arose because the CMA's simulation models confirmed that "some pricing algorithms can lead to collusive outcomes even where firms are each setting prices unilaterally." Moreover, the study found there were serious concerns about "hub-and-spoke" arrangements (*i.e.*, competitors coordinate with each other by each working with or through a central "hub" for the conspiracy), because firms could simply "adopt the same algorithmic pricing model" from vendors or even each other.

The current state of the law does not fully indicate whether these situations present legal problems. Although *respondeat superior* principles typically attach liability to companies for their employees' business-related acts, it is unclear whether AI could be considered an employee for such purposes, or even a conscious decision maker that could "agree" to collude. Also unclear is whether liability could or should attach to companies that are unaware of the pricing or other collusive decisions AIs independently make. Part of the purpose for AI programs is to automate pricing and other business decisions in an efficient, profit-maximizing way. If the AI effectively begins to collude with competitors, but does not alert human decision makers to that collusion, it is possible that companies might collude without anyone actually knowing they were doing so. Under certain readings of competition laws, there might be a strict liability treatment for such actions; but whether that is how courts would view the law and its application under these circumstances is currently unclear.

Another currently open question is what happens when human decision makers *do* become aware of AI's collusion and decide to support that collusion. Under tacit collusion principles, if that decision is made wholly within a company and does not involve any explicit or wink and a nod agreements with competitors to maintain the collusive *status quo*, then it may not be illegal. On the other hand, if competitors do communicate and acknowledge their AIs have begun to collude, yet do nothing about it, then more traditional conspiracy law may apply and the *ex post* agreement to support what was otherwise algorithmic tacit collusion might become actionable.

What all of this indicates is that AI-based collusion still is an open legal question; one that requires a case-specific analysis for risks. Furthermore, there is a spectrum of behavior from the human elements within a company that will affect the resulting legal analysis, even for situations that may have started off as relatively benign.

IV. What is the potential regulatory framework around AI collusion?

On January 19, 2021, the United Kingdom CMA provided a first look at a regulatory approach to AI collusion in a government publication entitled "Algorithms: How they can reduce competition and harm consumers." In the publication, the CMA goes far beyond the prior concerns articulated in

[1] https://www.gov.uk/government/publications/pricing-algorithms-research-collusion-and-personalised-pricing

2018 by providing a framework to approach, detect, and prosecute algorithmic schemes, and by marking the launch of a new CMA program to analyze these issues. The CMA approach is instructive to understand potential regulatory reform globally, and also informative to limit potential legal exposure in the United Kingdom—which is important given the extraterritorial reach of commercial activity on the internet.

First, the CMA concretely identified views on the necessity of understanding algorithmic collusion by articulating three primary concerns:

1. The increased availability of pricing data and the use of automated pricing systems can "facilitate explicit coordination" by making it easier to detect and respond to deviations and reducing the chance of errors or accidental deviations. Even simple pricing algorithms, with access to real-time data on competitors prices, could make explicit collusion between firms more stable.
2. Where firms use the same algorithmic system to set prices, including by using the same software or services supplied by a third-party, or by delegating their pricing decisions to a common intermediary, this can create a "hub-and-spoke" structure and facilitate information exchange.
3. There is a possibility of "autonomous tacit collusion," whereby pricing algorithms learn to collude without requiring other information sharing or existing coordination.

Significantly, in a potential departure from traditional concepts governing competition law, the CMA elaborated on the second and third concerns by claiming: "It is as yet unclear that competition authorities can object to hub and spoke and autonomous tacit collusion situations where, for example, there may not have been direct contact between two undertakings or a meeting of minds between them to restrict competition."

The CMA's suggestion that it may be "unclear" whether competition authorities can object where two firms do not have "direct contact" or even a "meeting of the minds" should be taken under serious consideration. As mentioned, similar to U.S. law, U.K. competition law requires the existence of an agreement or understanding between competitors. A framework lacking such a requirement will drastically effect any given firm's potential legal exposure, and provide a foundation for regulatory regimes, globally, to consider the same.

Second, in the event the U.K. abolishes such a requirement in hub-and-spoke or autonomous tacit collusion situations, firms may need to consider investigating internally given other aspects of the CMA publication. In particular, the CMA announced a new regulatory entity to gather information, and potentially enforce rules aimed at preventing algorithmic collusion: the Digital Markets Unit (DMU). The DMU will "implement a pro-competitive regime for digital markets," by understanding the "operation and effects of key algorithms and automated decision systems of significant firms." The CMA admitted "the risks of collusion in real-world markets is unclear due to a relative paucity of empirical evidence." Yet, the existence of a dedicated unit to gather information on automated decision system may provide increased awareness in the United Kingdom, and elsewhere, of practices that were previously unobserved, or even unknown by a given firm.

Third, on a related note, the CMA discussed potential formal investigations on suspicions a business's use of algorithms *may* have infringed consumer or competition law. And, the CMA disclosed specific remedial actions, including stringent disclosures on algorithmic systems, monitoring requirements, and risk assessments.

Despite the discussion on formal investigations and remedial powers, the CMA appears initially interested with information gathering in the short-term. For example, the publication concludes by noting, again, "there is relatively little empirical work on some specific areas of consumer and competition harms" and "we found gaps in work surrounding the operation and effects of automated pricing on collusion." The CMA, does however, caution firms to "ensure that they are able to explain how their algorithmic systems work."

The United Kingdom's announcement in the 2021 CMA publication provides one example of a regulatory agency identifying the potential problems with algorithmic pricing schemes, and in particular, potential legal exposure related to algorithmic tacit collusion or automatous algorithmic tacit collusion. Increased information gather as a result may invite increased scrutiny from competition regulatory agencies and enforcement. Additionally, the extraterritorial nature of the internet dictates that firms, globally, will need to comply with the potentially more restrictive laws of the United Kingdom. In a manner similar to the effects GDPR, a prohibition on autonomous collusion—even in the absence of agreement among humans—exposes any firm conducting internet business abroad to liability.

V. What should you be doing, and how can Quinn Emanuel help?

Given the current uncertainty surrounding this area of law, companies utilizing AI for any aspect of their competitive activities are well-advised to seek out legal advice during the AI's development and implementation phases. Legislators and regulators worldwide have taken ever greater interest in the opportunities for collusion AI potentially represents. Therefore, a prudent strategy is to minimize risks before they even arise.

Quinn Emanuel is well-positioned to provide this sort of advice and, if needed, both defend and prosecute these sorts of actions. In addition to its worldwide competition practice (particularly in the U.S., E.U., and U.K.), Quinn Emanuel also is at the forefront of AI litigation and intimately understands the developments in that law. By getting us on your side, you will reduce your company's risk of liability even while implementing new and better AI to help your business thrive.

***

If you have any questions about the issues addressed in this Client Alert, or if you would like a copy of any of the materials we reference, please do not hesitate to contact us:

Adam Wolfson
Email: adamwolfson@quinnemanuel.com
Phone: +1 213-443-3084

Steig Olson
Email: steigolson@quinnemanuel.com
Phone: +1 212-849-7152

Kevin Teruya
Email: kevinteruya@quinnemanuel.com
Phone: +1 213-443-3226

Stephen Mavroghenis
Email: stephenmavroghenis@quinnemanuel.com
Phone: +32 2 416 50 03

Debra Bernstein
Email: debrabernstein@quinnemanuel.com
Phone: +1 404-654-3528

Boris Bronfentrinker
Email: borisbronfentrinker@quinnemanuel.com
Phone: +44 20 7653-2090