Freshfields Bruckhaus Deringer

Pricing algorithms: the digital collusion scenarios

The classic digital cartel

This category serves as a reminder that price fixing cartels are illegal, irrespective of the means by which they are implemented or operated. This is the digital equivalent of the smoke-filled room agreement: algorithms are used intentionally to implement, monitor and police cartels. In this scenario, humans agree to collude and machines execute the collusion, acting as mere intermediaries or messengers.

An example is the so-called *Poster Cartel* case, which made David Topkins, the founder of Poster Revolution, the first senior manager from an e-commerce business to be prosecuted under antitrust law by the US Department of Justice. David Topkins and his co-conspirators adopted specific pricing algorithms that collected competitors' pricing information, with the goal of coordinating changes to their pricing strategies for the sale of posters on Amazon Marketplace.

From a legal perspective, the use of algorithms to help execute the cartel's task has the same effect as a cartel executed by humans: humans are guilty for agreeing to fix prices, while the computer merely facilitates the task which humans would otherwise have carried out. Or as Vestager put it: 'companies can't escape responsibility by hiding behind a computer program.'

From a practical perspective, users of pricing algorithms should be aware that sharing information about the algorithm itself (its structure, workings etc.) publicly or with competitors might be considered illegal as it would allow others to draw conclusions about how prices are/will be calculated. In that sense, the algorithm could function as a 'messenger' of competitively sensitive information. Companies will have to be careful to avoid information about their algorithms leaking. Even if it can be shown that the leak was inadvertent, competition authorities might require companies to amend their algorithms or adopt new ones in order to prevent collusive behaviour from arising as a result of the leak.

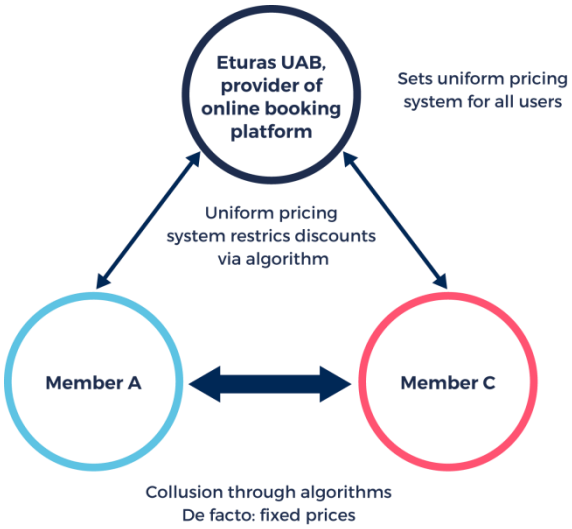
The (inadvertent) hub-and-spoke scenario

Online retailers using third party provider's algorithms might find themselves facing cartel allegations without, in fact, having intended participation in a cartel. In this scenario, various industry players (the spokes) use the same third-party provider's (the hub's) pricing algorithm to determine the market price and/or react to market changes. Unlike in the first scenario, the algorithm is not necessarily merely a means to carry out a cartel, but it is the use of the same pricing algorithm by competitors to monitor prices that leads to the (possibly unintentional) fixing of prices.

The recent *Eturas* case serves as a reminder that hub-and-spoke agreements also exist in the online world. Here, the administrator of a Lithuanian online travel booking system sent an electronic notice to its travel agents, declaring a new technical restriction that put a cap on discount rates. The Court of Justice of the European Union made clear that travel agents who knew of the message could be presumed to have participated in a cartel, unless they publicly distanced themselves from the

message. The Court confirmed that actual knowledge of the administrator message was required for an infringement to exist, but knowledge could be inferred from 'objective and consistent' indicia.

Figure 1. Eturas hub-and-spoke



Thus, where firms independently sign up to using a platform's algorithm, knowing that other competitors are using the same algorithm and that the algorithm fixes prices at a certain level, they can be held to have engaged in classic hub-and-spoke behaviour.

In light of the *Eturas* judgment, businesses using third party algorithms will need to ensure online communication channels (emails, amendments to terms and conditions etc) are effectively monitored to avoid inferences of collusion (eg where a jointly used algorithm starts setting prices for all of its users). The precise scope of the 'objective and consistent' indicia remains unclear. Deliberately turning a blind eye is therefore not recommended. Developers of algorithms should also be wary of the effects of their algorithms, so as to steer clear of allegations of engaging in vertical or facilitating horizontal collusion.

M2M communication and self-learning algorithms

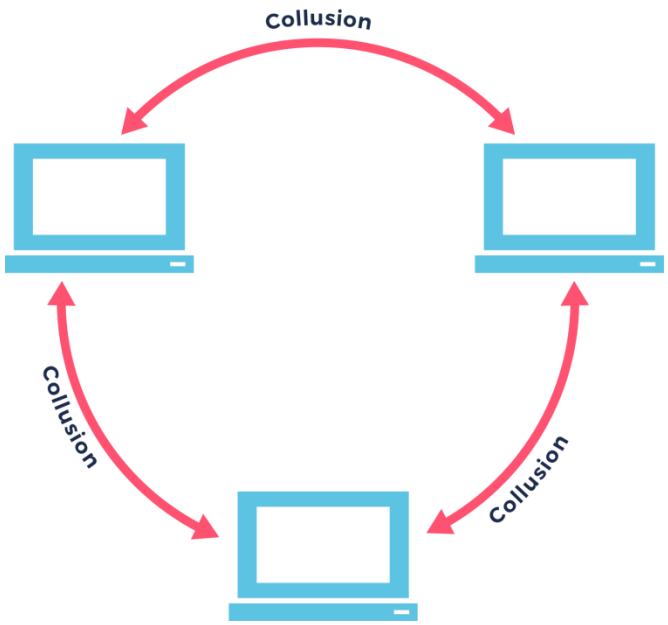
What happens if algorithms figure out ways to coordinate prices without their developers / users being aware of it? That is the question central to this third category in which Artificial Intelligence (ie the increasing ability of algorithms to make autonomous decisions and learn through experience) leads to an anticompetitive outcome with no anticompetitive intent or meeting of minds between humans at all.

Where algorithms are programmed to communicate and exchange information with competitors' algorithms, it is likely that they will be treated as an extension of human will. Even though the 'meeting of minds' takes place at machine level, it was, arguably, initiated at the human level.

Another question is how situations should be treated where the exchange of information between algorithms was not part of a human plan, but the programmers have (unintentionally) omitted to implement the necessary safeguards to prevent the exchange from happening. Commissioner Vestager alludes to this when she states that 'what businesses can and must do is to ensure antitrust compliance by design. That means pricing algorithms need to be built in a way that doesn't allow them to collude.'

Vestager's comment suggests that authorities may challenge instances where companies have failed to build in sufficient safeguards into their algorithms to prevent them from engaging in illegal activity by 'agreeing' with rival firms' systems to fix prices.

It may indeed be possible to command an algorithm not to fix prices, but what if through self-learning and experimenting with different solutions, including legal forms of coordinated interaction, the algorithm in its quest to optimise profit finds that the best strategy would be to coordinate prices regardless? Here, it is machine self-learning that leads to collusion, while the humans that have programmed or are operating the machines are not aware whether, when or for how long the collusion has been going on.



Vestager's reaction is as follows: 'what businesses need to know is that when they decide to use an automated system, they will be held responsible for what it does. So they had better know how that system works.' But to what extent can humans really be held responsible for their algorithms' actions which they maybe knew was one of many possibilities, but certainly not probable? Or as the UK CMA's top official David Currie put it: 'how far can the concept of human agency be stretched to cover these sorts of issues?'

The general principle under EU law is that companies will be held liable for any anti-competitive practices of their employees, even if they can show that they have used their best efforts to prevent such behaviour (eg by implementing a state of the art compliance program). Vestager's statements suggest that this principle will be extended to algorithms: where a company uses algorithms to set prices, it is responsible for any resulting competition risks and will be held strictly liable.

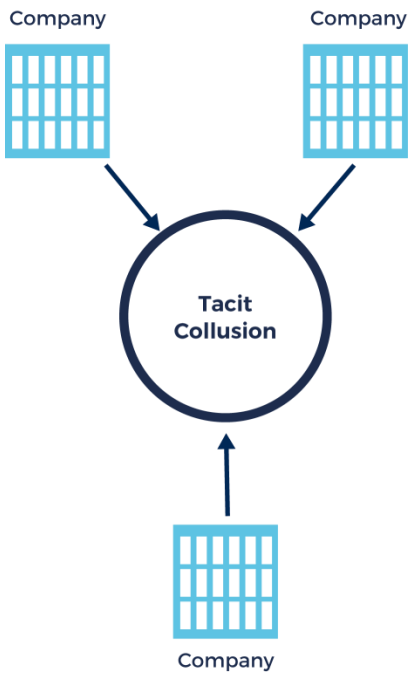
Whilst the idea of algorithms getting together and colluding may still sound like science fiction, businesses need to be aware that they may be held responsible for whatever the algorithms they develop or use do. Companies should start thinking about the practical implications of this and the technical ways in which to prevent M2M collusion from happening.

The tacit algorithmic collusion scenario

This scenario works on the assumption that the increasing use of pricing algorithms combined with growing market transparency results in tacit collusion. Under current rules, the tacit collusion scenario (ie 'conscious parallelism' which establishes itself without a need to collude actively) does not lead to an antitrust offence being committed, so companies do not have to worry about it just yet. Nevertheless, regulators are already discussing this and it is important that businesses are aware of the issues, so as to be able to engage actively with regulators, where possible, and be prepared for and/or influence developments in this area.

Dynamic algorithmic pricing is efficient and clearly yields a competitive advantage, which fewer companies will want to or can miss out on. With more and more companies adopting pricing algorithms and more sellers posting their current prices, more market data becomes accessible and market transparency increases. A market where all firms unilaterally adopt their own pricing algorithm, accessing their rivals' real-time pricing and adjusting to each other's prices within seconds or even in real time can constitute a breeding ground for tacit collusion. If one firm increases prices, its rivals' systems will respond immediately. This normally happens without the risk that enough customers will realise and be able to move to other sellers. On the flip side, where a firm decreases its prices, competitors will also adjust theirs straightaway, so that, ultimately, there is no competitive gain in and hence no incentive to offer discounts.

Figure 2. Use of pricing algorithms leading to tacit collusion



The risk then arises that market players find a sustainable 'supra-competitive' price equilibrium (ie an algorithm-determined price which is higher than the price that would exist under competitive market conditions).

Importantly, monitoring your competitors' prices and reacting to any competitor's price change (conscious parallelism), is not in itself unlawful. Thus, whilst real-time monitoring of competitor prices and dynamic algorithmic pricing might have an anticompetitive effect, absent evidence of any form of agreement or explicit collusion among competitors, competition agencies – at least as things currently stand – lack the legal basis for intervention. As put by the German and French authorities in their joint report: '…prosecuting such conducts could prove difficult: first, market transparency is generally said to benefit consumers when they have – at least in theory – the same information as the companies and second, no coordination may be necessary to achieve […] supra-competitive results.'

Some commentators have suggested that legislation targeting 'abuse' of excessive market transparency is conceivable. Alternatively, authorities might try and address the issue by preventing the creation of an excessively transparent market, in the same vein as existing competition law prohibits mergers that make tacit collusion more likely.

However, arguably, any attempts at prohibiting conscious parallelism or (excessive) market transparency are likely to raise more questions than they answer. How should the threshold for intervention be defined? There is general agreement that transparency is in principle pro-competitive in that it allows consumers to easily compare competing offers, unless the market becomes so transparent that it 'tips' into tacit collusion. It would be very difficult, or even impossible, for any regulator to reliably predict this 'tipping point'. Moreover, what would be the remedy in markets which are classified as susceptible to a risk of tacit collusion? Can the use of pricing algorithms in certain markets be banned altogether, depriving consumers of the many benefits that these algorithms entail?

Pricing Algorithms and Patents

Any developments in relation to pricing algorithms might go beyond just antitrust considerations and could impact other areas, such as IP law. As discussed, companies should not be making information on their own pricing algorithms available. The less competitors know of/about each other's algorithms, the more difficult it becomes to accuse them of collusion. By patenting their pricing algorithms, companies would, however, be revealing information about their algorithms (also to competitors), thereby making arguments around knowledge/awareness of competitors' strategies more likely. This is a reason for companies not to seek patents for their pricing algorithms. On the flip side, lack of patent protection might leave businesses vulnerable to patents from third parties that cover the same activity. Either way, companies should tread carefully when thinking of protecting their pricing software by way of a patent.

Freshfields Bruckhaus Deringer