Bloomberg Law

Professional Perspective

Antitrust Compliance and Pricing Algorithms

Creighton Macy and Dan Graulich, Baker McKenzie, and Matthew Bester, Accenture

Antitrust Compliance and Pricing Algorithms

Contributed by Creighton Macy and Dan Graulich, Baker McKenzie, and Matthew Bester, Accenture

Antitrust enforcement officials in the U.S. and EU are watching developments surrounding the use of pricing algorithms and artificial intelligence. One area in particular that has drawn attention is the emerging use for AI to combine data and analytics to more accurately price products. Of course, competitive intelligence gathering is a fact of life in business, and many companies have compliance policies to deal with antitrust risks that can arise when handling such information. However, what is (somewhat) new is that pricing algorithms and AI can further automate and accelerate the process through which companies set prices and gather information. But do these new technologies create unique antitrust risks?

The short answer is no. Luckily, companies don't need to look too far to see how antitrust authorities have confronted these issues. Antitrust enforcers are using time-tested approaches to questions concerning very new technology. For corporate compliance teams, that means that the safeguards are similar to those you would encounter in other familiar contexts.

This article explores real-world examples and lays out key corporate compliance considerations that are likely to arise when using these technologies. We also look at how enforcers are evaluating the issues surrounding pricing algorithms and the importance they have placed on applying traditional frameworks in analyzing these emerging technologies.

Defining Algorithms

An algorithm is a set of instructions that can do things like automate a specific task or analyze complex sets of data. For instance, compared to traditional analytic methods, pricing algorithms can set prices faster and more dynamically. They can also be used to track and analyze a wide range of factors in real time—such as other companies' prices, product availability, and consumer purchasing patterns.

There are two broad contexts where pricing algorithms are commonly used. The first is using pricing software to monitor or adjust pricing. For example, a retailer may use algorithms to adjust prices based on what competing sellers charge, whereas a distributor might use online tools to monitor other distributors' prices. The second is where a pricing algorithm is sourced by a third party. We examine each scenario in turn.

Scenario 1: Using Software to Monitor or Adjust Pricing

Sellers and manufacturers regularly use price-tracking technologies to serve important business goals. So when can antitrust issues arise?

Using algorithms to facilitate unlawful agreements: Serious antitrust risk occurs where competing online sellers agree to use the same pricing algorithm to coordinate their prices. The most well-known example is the Topkins case in which the Department of Justice Antitrust Division and UK Competition and Markets Authority investigated and charged several online sellers with using the same pricing algorithm, designed by one of the defendants, to coordinate prices across the sellers for posters sold through Amazon Marketplace. Topkins wrote computer code that other poster sellers agreed to use for their algorithm-based price-setting software. This example, of course, represents the traditional types of conduct that one should expect the DOJ to pursue in any case—the algorithm simply took the place of human-based communications to coordinate prices among competitors.

Risks can also rise in the distribution context—particularly in Europe, where the European Commission takes a stricter approach toward distribution restrictions than the U.S. For example, in *Consumer Electronics*, the EC fined, in four separate decisions, consumer electronics companies for fixing online resale prices. According to the EC, each company used sophisticated price-monitoring tools to identify those online retailers that deviated from the company's requested prices. While each company's individual decision to use price-monitoring tools was not in and of itself illegal, the EC observed that these tools allowed each company to intervene swiftly when it saw price decreases and more readily effectuate resale price maintenance agreements (which are essentially per se illegal offenses in the EU) with its online retailers.

Companies using pricing technologies to signal pricing plans to competitors: Disclosing pricing plans, particularly future price increases, can draw scrutiny if they are otherwise commercially sensitive and of little utility to customers. For example, in the 1994 case of Airline Tariff Publishing, the DOJ alleged that six airlines pre-announced proposed fare prices through a computerized clearinghouse (although not algorithm-based software) to coordinate prices on competing routes and used coded language in fare basis codes and footnotes to communicate with other airlines about fares.

In agreeing to settle the case, the airlines agreed not to pre-announce fare increases unless the company had launched a consumer advertising campaign and to only communicate objective identifying information through the fare basis codes. In addition to the risks that arise from intentionally using pricing technologies to signal business plans to competitors, it is important for companies to carefully review the types of pricing information that they disclose through their use of pricing software—particularly if it is prospective.

Failure to monitor self-learning algorithms: Because most computer-based pricing technologies (like those described above) are human-led (i.e., they are designed to execute specific tasks), it is common when discussing pricing algorithms to focus primarily on the issues companies will face in how they design and use the algorithm in practice. But the advent of AI poses different challenges since these technologies may possess self-learning capabilities that may not be entirely foreseen by the developer. Although the technical requirements for monitoring employees may differ from those associated with monitoring algorithms, similar principles to those discussed above may apply.

Key Takeaways

Conduct that is illegal if carried out by people is illegal if implemented by a machine or algorithm: As demonstrated by *Topkins*, the mechanism used to facilitate an agreement is typically of less relevance than the agreement itself. And as demonstrated by *Airline Tariff Publishing* and *Consumer Electronics*, antitrust authorities will pay particular attention to the use of industry-wide tools and instances where there are fewer market participants that regularly use identical or highly similar pricing technologies.

Counsel should pay close attention to how pricing software is developed and put to use: It is important at both the design and implementation stage that counsel communicate with both engineers and sales personnel about the types of commercially significant information that may be disclosed through the use of pricing software. In any event, it is important to document as these tools are developed how pricing software is used and the business justification for such use. Companies should also generally avoid publicly disclosing how their pricing tools are used when making pricing decisions and the details underlying such decisions.

The type of compliance measures needed may vary depending on the algorithm's self-learning capabilities: Compliance policies should always be tailored to address the risks posed by the technology at issue. For any pricing technologies with self-learning capabilities, it would be prudent from a risk mitigation perspective to assess actual impact on prices and potentially set up reporting for employees tasked with tracking how such tools are used in practice.

Scenario 2: Third Parties that Offer Pricing Algorithm Services

Third parties that offer pricing software to multiple users face a different set of legal challenges. While these technologies offer valuable benefits to customers, the key antitrust risk for third-party controlled algorithms involves managing competitively sensitive information (like disaggregated pricing and transaction information) generated by users. The antitrust implications therefore depend on how the technology is used and the technological or contractual safeguards in place designed to protect users' competitively sensitive information.

For analytical convenience, we focus on three kinds of pricing tools:

Individualized Pricing Tools: Pricing tools are often engineered by specialist technology companies and can be offered to businesses operating in the same market. While there is a possibility that multiple companies can decide to use identical or similar pricing tools, these tools generally raise less antitrust risk to the extent customer purchasing decisions are made on an independent basis and the types of data fed to the pricing tools differs.

Nonetheless, sellers of individualized pricing tools can take steps to minimize potential conflicts of interest between users and limit their potential antitrust exposure. For example, the seller could offer customers greater customization by building and offering tools that prevent user data from being disclosed or accessed by other users who purchase the tool. Similarly, the seller could include contractual provisions like firewalls and non-disclosure commitments to protect customers' confidential or proprietary information.

Pricing Aggregators: Pricing aggregators are metasearch tools that can carry out a number of searches and identify price points for specific goods and services. Because an aggregator is a single tool that is made available on a common basis, there is a risk that the tool could facilitate exchanges of competitively sensitive information among users. For example, in 2016 the DOJ issued a Business Review Letter to Mystic Holdings that analyzed its "Amadeus" pricing aggregator, which calculated postage, packaging, and transportation scenarios for commercial mailing logistics providers.

In stating that it would not bring an enforcement action, the DOJ concluded that Mystic had implemented numerous safeguards that would prevent anticompetitive effects and protect against unlawful sharing of subscribers' competitively sensitive information. In particular, DOJ cited Mystic's representation that it would maintain firewalls and encrypt certain competitively sensitive data to ensure that any information uploaded by a user could not be accessed by other subscribers. Mystic also represented that it was contractually bound not to share the information with third parties and that employees would be held to a strict standard of confidentiality. Finally, the DOJ highlighted that the tool would be offered on a non-exclusive basis.

Platform-based tools that facilitate user transactions: Pricing algorithms may be used to "match" different sets of users and set the prices at which users transact. A particularly notable example that has generated significant attention amongst antitrust practitioners is ride-sharing. Some have argued that the ride sharing services involve "joint" determination of prices among users since each driver that signs up agrees to charge the price set by the mobile app knowing that all other drivers who sign up will do the same. Indeed, one U.S. district court allowed price-fixing claims against the former chief executive of Uber to survive a motion to dismiss before the case was later sent to arbitration after Uber intervened (*Meyer v. Kalanick*). However, this view doesn't account for the matching function and efficiencies inherent to a ride sharing app's implementation of a common pricing technology, which itself is unilaterally designed, developed, and implemented by the platform operator (and not the users).

The Luxembourg Competition Council's 2018 analysis of Webtaxi, an app-based taxi booking system, illustrates this point and the importance of paying attention to an app's technical features when analyzing potential efficiencies associated with a pricing algorithm. In conducting an in-depth analysis of Webtaxi's platform, the Council recognized that the app's use of a uniform fare was "indispensable" to maximizing the number of taxi bookings for both technical and practical reasons. Specifically, the app sets prices automatically based on users geolocation without input from users, which ensures that largest number of riders are matched with drivers in the quickest manner possible.

Otherwise, users would be required to individually negotiate fares each time a potential match is made, which in turn would interfere with the platform's ability to match users based on real time utilization of the app. Accordingly, the Council determined that the benefits of a uniform fare outweighed the harms to riders, including reduced wait times and lower risk of additional fare increases due to traffic jams. As such, the operation of the price-setting mechanism, which was claimed to be illegal in the Meyer case, became a central point in Webtaxi's successful defense and communicating the significant benefits to users that were generated through the platform.

Key Takeaways

Third parties face unique compliance challenges: Algorithm developers and platform operators should be aware of the risks that can arise from their ability to access confidential information among competing customers. A holistic approach is also necessary to understand the antitrust risks associated with sourcing algorithms from a third-party provider. In any event, software engineers and personnel tasked with managing pricing tools need to understand the safeguards to protect information contributed by users as well as the potential antitrust implications associated with making design or operational changes.

Explicit design features, internal safeguards, or both may be necessary to mitigate risk: The DOJ's business review letter to Mystic indicates that maintaining confidentiality around customer information can significantly reduce antitrust exposure. The Amadeus example shows that safeguarding customer data and setting up firewalls to prevent third parties from accessing the data is a key risk mitigation measure from a compliance perspective. Nonetheless, depending on the business model, protecting customer information may not be enough. Additional technological safeguards, such as explicit design features to prevent pooling of competitors' data or internal safeguards such as compartmentalizing staff through firewalls, may be necessary depending on the business model and underlying market conditions.

Documenting business justifications and consumer benefits can go a long way: Webtaxi successfully defended itself by detailing the technical features of its app and providing data on the additional rides that took place as a result of the app's integrated features. Because Webtaxi was able to explain how the technology involved improved the operation and value of its app for drivers and riders, the Luxembourg Competition Council found that the benefits of Webtaxi's uniform mechanism for setting fares outweighed the potential harms to users.

Beyond Webtaxi, justification and accountability for the use of algorithms is likely to remain a theme in future legal proceedings, which will likely require documentation of both design features and effects on users. When dealing with third parties, the need for documentation is stronger—a company must be able to show that it carried out its due diligence and had the correct contractual and structural measures in place.

Future Enforcement Approach

Although U.S. and EU antitrust enforcement officials have recognized the potential antitrust challenges presented by pricing algorithms, they have also recognized the importance of relying on familiar frameworks in analyzing these technologies. For example, the EC explained in its note submitted to the June 2017 OECD roundtable on Algorithms and Collusion that, "[t]o a large extent, pricing algorithms can be analyzed by reference to the traditional reasoning and categories used in EU competition law."

More recently, in a joint report on "Algorithms and Competition" published in Nov. 2019, the French and German antitrust agencies concluded that, so far, the current antitrust toolbox and case law is sufficient to address possible concerns. Similarly, the DOJ and FTC concluded in their note to the OECD that, "[a]bsent concerted action, independent adoption of the same or similar pricing algorithms is unlikely to lead to antitrust liability even if it makes interdependent pricing more likely."

Antitrust enforcement officials have also indicated the need to take a cautious approach that views algorithms primarily as a compliance issue. In August 2019, Margrethe Vestager, the European Commissioner for Competition, discussed plans to put forward a proposal for ethical guidelines outlining Europe's approach to artificial intelligence within the first 100 days of her new term. With respect to pricing technologies specifically, she previously commented in a March 2017 speech that "[w]e certainly shouldn't panic about the way algorithms are affecting markets." Instead, she advised companies to focus their attention primarily on the issue of "compliance by design," which means building "pricing algorithms … in a way that doesn't allow them to collude." This approach is consistent with that outlined in the EC's note to the OECD, which explains that, "[l]ike an employee … an algorithm remains under the firm's control, and therefore the firm is liable for its actions."

U.S. antitrust enforcement officials have similarly focused on the risk posed by algorithms that are programmed to collude while emphasizing the need for a tailored enforcement approach. For example, in a November 2018 speech before the Federal Institute of Telecommunications, Makan Delrahim, the Assistant Attorney General of the DOJ Antitrust Section, explained that the Division was continuing to work on ensuring that it "ha[s] the tools to detect and prosecute any illegal agreement, no matter the technology used to enter the agreement or implement it." At the same time, he cautioned that, "[w]hile algorithms can be used to facilitate price fixing, it is important to keep in mind that they are not inherently anticompetitive. Indeed, algorithms are an important part of the digital economy and can account for great efficiencies that benefit consumers."

Similarly, at Nov. 2018 Federal Trade Commission hearings on the topic of the competition implications of algorithms and AI, Bruce Hoffman, then-Director of the FTC Bureau of Competition, stated, "at this early stage in the development of these technologies, it is very difficult to see where this is going to go in the next 10 or 20 years … [w]e need to be very careful not to regulate or enforce without [an] empirical, fact-based, theoretical framework."

Conclusion

While pricing algorithms and AI are new, the analytical framework to judge their competitive impact is not. Yet this framework is inherently flexible enough to adjust to emerging industry risks.

Accordingly, the lesson for companies is that the antitrust issues surrounding algorithms are not abstract; rather, they are a matter of antitrust compliance. As former Acting FTC Chairperson Maureen Ohlhausen explained, "[e]verywhere the word 'algorithm' appears, please just insert the words 'a guy named Bob' …. If it isn't ok for a guy named Bob to do it, then it probably isn't ok for an algorithm to do it either." Just as antitrust trainings and reporting procedures would be sensible to implement for someone managing a customer rewards program, it is important to have antitrust compliance procedures and policies in place for pricing algorithms.

The authors would like to thank Grant Murray and Cem Ucan for their insight with respect to this article.

