

AI and Algorithms: FTC Issues Guidance for Companies Amid Heightened Scrutiny

April 23, 2020

Even before the COVID-19 crisis, artificial intelligence and algorithms, particularly in the context of pricing, were a focus of the Federal Trade Commission and the Department of Justice's Antitrust Division. With the COVID-19 pandemic shining a spotlight on online platforms and sellers using algorithms to set prices, it is particularly important that companies are aware of the latest guidance from the agencies on how to ensure that use of AI does not violate either antitrust or consumer protection law.

In the midst of the pandemic on April 8, the director of the FTC's Bureau of Consumer Protection issued guidance on the use of artificial intelligence and algorithms, which advises that "the use of AI tools should be transparent, explainable, fair, and empirically sound, while fostering accountability."

On the antitrust front, agency speeches and enforcement actions provide insight on how the agencies will assess use of AI and algorithmic pricing.

FTC consumer protection guide requires AI tools to be transparent, fair and empirically sound, and that decisions be communicated to the consumer

FTC guidance is primarily aimed at helping businesses avoid concerns about misleading consumers, illegal discrimination or violation of the Fair Credit Reporting Act (FCRA), the last of which may apply to companies that assemble consumer information to use for decision-making about eligibility for credit, employment, insurance, housing or similar benefits and transactions.

That said, the guide has implications for use of algorithms and AI in all industries. For example, the guide specifically highlights healthcare AI as an area where companies should exercise caution, noting that a recent algorithm developed "with good intentions – to target medical interventions to the sickest patients – ended up funneling resources to a healthier, white population, to the detriment of sicker, black patients," violating the Equal Credit Opportunity Act (ECOA).

The new guidance focuses on four major issues that companies marketing or selling to consumers should consider when designing, implementing and using AI: the algorithm should be (1) transparent about the use of AI; (2) fair; (3) empirically sound; and (4) any decisions based on the algorithm should be communicated to the consumer.

- **Transparent about the use of AI.** The guidance emphasizes that companies that mislead consumers about the use of automated tools, such as AI chatbots that deceive consumers into believing they are communicating with a live person, could face FTC enforcement. The guidance highlights the FTC's 2017 Ashley Madison enforcement action based in part on allegations that the website used fake "engager profiles" and its 2019 Devumi enforcement action that alleged that the company sold fake followers, subscribers, views and "likes" to users of social media platforms. The guidance also notes that the FCRA may require a company to provide an "adverse action" notice and the right to correct inaccurate information, if the company relies on information, such as credit history, criminal records, shopping history or the like to automate decision-making about eligibility for credit, employment, insurance, housing or similar benefits and transactions.
- **Fair.** The guidance advises that both inputs and outcomes are important in determining whether an algorithm illegally discriminates against a protected class in violation of federal equal opportunity laws, including the ECOA, which is enforced by the FTC and prohibits credit discrimination. For example, algorithms may be deemed discriminatory in cases where the

inputs to the model include ethnically based factors, or proxies for such factors (e.g., zip codes), as well as in cases where a facially neutral model results in a disparate impact on a protected class. The guidance recommends that “companies using AI and algorithmic tools should consider whether they should engage in self-testing of AI outcomes, to manage the consumer protection risks inherent in using such models.”

- **Empirically sound.** The guidance highlights companies’ obligation to ensure AI models provide the maximum possible accuracy for consumer reports and provide consumers with access to their own information. In particular, the FTC highlighted the FCRA’s requirement that companies ensure that their algorithms are “empirically derived, demonstrably and statically sound,” where the company is a “consumer reporting agency.” The FTC argues this requirement may apply to companies using algorithms to generate data that may be used to make decisions about consumer access to credit, employment, insurance, housing, government benefits, check-cashing or similar transactions.
The guidance also noted the value of “outside, objective observers” to “independently test the algorithm.” In a panel held after release of the guidance, the director of the FTC’s Bureau of Consumer Protection stressed the value of outside validation to confirm that algorithms are accurate and non-discriminatory. He explained: “We would like to see companies doing that kind of [outside] validation [of their algorithms] themselves, and not waiting for a third party to sort of blow the whistle on them. This is the kind of expectation that financial regulators and the FTC have imposed on lenders for years – the requirement they validate, and re-validate, and ensure that their models remain statistically sound and empirically derived.”
- **Clearly communicate decisions to the consumer.** The guidance suggests that when companies rely on algorithms to deny consumers something of value or assign risk scores (e.g., assignment of a credit score, denial of a business loan or housing application), they must be in a position to (1) disclose the key factors that impact the algorithm’s decision making process and (2) explain to the consumer why the algorithm arrived at a particular result. The guidance cited CompuCredit, a subprime credit marketer, as an example of a company that violated the FTC Act by deceptively failing to disclose that its algorithm reduced consumers’ credit limits based on their behavior, including using their credit card at nightclubs and massage parlors. While this type of disclosure is mandated in the credit industry, the FTC bureau director argues that it is best practice to implement such a policy regardless of the industry. Indeed, companies that are subject to GDPR must already adhere to similar disclosure, transparency and accuracy requirements. For more information on GDPR compliance, see Cooley’s [GDPR resource page](#).

The new guidance recommends methods that companies can employ to reduce risk, including (1) ensuring data sets are based on non-discriminatory inputs, accurate and up to date; (2) proactively implementing safeguards to prevent misuse use of AI; and (3) ensuring accountability by, for example, hiring independent observers to periodically test consumer facing algorithms to ensure they produce non-discriminatory outcomes and are empirically sound. Companies should also keep in mind that the FTC’s guidance is limited to ensuring compliance with laws and regulation within the FTC’s purview. Companies that use AI may need to adopt additional policies and procedures in order to comply with other US and international laws and regulations that govern the use of AI and algorithms.

Antitrust considerations for algorithmic pricing

In today’s online marketplaces (also known as third-party seller platforms), it is common for sellers to set pricing using such technology-assisted pricing tools, replacing the traditional model of individual business executives making pricing decisions. AI and pricing algorithms have generated substantial attention in antitrust circles, including [in the context of the COVID-19 pandemic](#), with particular attention on price gouging. While dynamic pricing tools provide the potential for tremendous efficiencies and lower prices, if not carefully configured or monitored, these pricing tools may automatically increase pricing during a time of supply and demand disruption, like the COVID-19 pandemic. The result may be price spikes that sellers may not be aware of if they are not closely following their products on the marketplaces on which they sell.

As the ABA Antitrust Section noted in comments before the recent FTC Hearings on Competition and Consumer Protection in the 21st Century, algorithmic pricing can enhance competition by facilitating rapid responses to changing competitive conditions and customer demand. Enhanced price discovery and dissemination – the crucial function of the price system itself – is likely to make markets more efficient and competitive.

While some have suggested that the use of algorithms may facilitate collusion and make cartels more stable, senior government officials have noted that while antitrust authorities need to be vigilant, existing rules can be used to control misuse and the concerns raised are alarmist. Computer-determined pricing may be susceptible to coordination, just as human-determined pricing can be, and antitrust law is equipped to confront this issue.

For example, the antitrust agencies have brought enforcement actions against:

- A group of airlines that used a shared online reservation system to communicate with each other and set airline fares
- E-commerce sellers that agreed to adopt a complex pricing algorithm in order to avoid undercutting each other's prices online

Antitrust enforcers have said that they have the technological capacity to identify price fixing or other illegal conduct through algorithms and have hired "technologists" to assist in their investigations. Enforcers are paying close attention to subtle uses of technology-aided pricing to coordinate conduct, including through sharing pricing information with intermediaries, which then develops an algorithm for use by each to maximize prices. Even without direct communication between sellers, enforcers have suggested that this conduct may be subject to challenge as a hub-and-spoke conspiracy.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our [legal notices](#).

Key Contacts

Megan Browdie Washington, DC	mbrowdie@cooley.com +1 202 728 7104
Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.