Hashed & Salted | A Privacy and Data Security Update
September 2025

A Cautionary Tale About Algorithmic Pricing Software

The use of algorithmic pricing software, including dynamic and competitive pricing, raises fairness, antitrust and privacy concerns when the data is based on personal, nonpublic or competitively sensitive data. Businesses must carefully manage these pricing tools and the associated data input sources to comply with consumer protection, privacy and antitrust laws, as well as to stay aware of any discriminatory or collusive pricing practices.

How Is Personal Data Used For Pricing?

Dynamic pricing is increasingly used in ride-sharing and delivery platforms, event ticketing, real estate, travel and hospitality, and e-commerce. While pricing may be impacted by market pricing (e.g., surge pricing), personal data can also factor into the pricing decision. Personal data is generally defined as any data or information that relates (or could reasonably be linked) to an identified or identifiable individual. Examples of personal data commonly used for dynamic pricing are name and contact information (such as email address or phone number), location data (such as physical address or geolocation), browsing and purchase history, account information, demographic details and online identifiers. An individual's location, preferences and shopping habits are all useful in helping companies personalize their pricing.

When pricing intelligence software utilizes personal data, the software (and the business using the software) must comply with privacy rules and ethical standards to protect consumer information and prevent discriminatory pricing.

On Our Radar: Select State-Specific Requirements

New York's Algorithmic Pricing Disclosure Act

New York's Algorithmic Pricing Disclosure Act, which became effective July 8, 2025, applies to businesses using algorithms to dynamically set prices in New York based on consumers' personal data. As of this article's publication date, enforcement is still on hold due to a legal challenge from the National Retail Federation (NRF), with a general stay of enforcement issued on July 14, 2025. The U.S. Chamber of Commerce has since filed an amicus brief in support of the NRF. Oral arguments on the lawsuit should take place soon, and we are monitoring updates regarding a final ruling. Even if the NRF's challenge is

Attorney Advertising

denied, enforcement cannot begin until 30 days after the final court order. New York's attorney general has indicated that she will not enforce the act or investigate potential violations prior to the enforcement date.

Disclosure Requirement: Companies in New York using automated or algorithmic systems to set or adjust prices using consumers' personal data must clearly and conspicuously disclose to consumers that algorithmic pricing is used by including the following disclosure in connection with the price: "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA."

Ban on Discrimination: The New York law also prohibits using personal data relating to protected classes (e.g., race, gender) that would result in discriminatory treatment or different pricing based on those characteristics.

Failed Advancement of Legislation in California

California has recently suspended its review of the Surveillance Pricing Protection Act (AB 446), which aimed to enhance consumer protection through transparency and antidiscrimination measures. As of this article's publication date, the bill failed to advance and will not move forward in 2025. If it had passed, the law would have had the following features:

Ban on Surveillance Pricing: AB 446 would ban "surveillance pricing," which is generally defined as setting pricing for a specific consumer (or a group of consumers) using personal data such as geolocation, web browsing history or inferences about personal characteristics collected through cookies and similar tracking technologies. AB 446 would also prohibit businesses from charging different consumers (or groups of consumers) different prices for the same product or service.

Ban on Discrimination: AB 446 would also make it illegal for businesses to use personal data, such as geolocation or web browsing history, for discriminatory pricing strategies.

AB 446 may return for consideration in a future legislative session; however, any advancement of the bill would require committee approval and we likely will see changes to the text.

What Companies Should Consider in an Ever-Evolving Regulatory Landscape

While these and other state bills are pending, companies should:

- Evaluate whether they are using algorithmic or other dynamic pricing models.
- Determine whether those models are based on market conditions or personal data.
- Where personal data is used, determine whether the collection and use of personal data for this purpose has been properly disclosed (and note that certain sensitive categories of personal data require consent prior to collection in certain states).
- Identify any risks of discrimination if race, gender or other protected class data is relied on by the pricing model.
- Consider whether an impact assessment should be conducted, as the use of personal data for dynamic pricing may be considered "automated decision-making" with significant effects.
- Determine what rights the company may be required to offer to consumers based on the nature of the data used, the location of its consumers and the laws that may apply to its activities.

Antitrust Concerns With Algorithmic Pricing

Whether and to what extent algorithmic price comparison tools violate U.S. antitrust laws is unsettled and quickly evolving. A number of theories for imposing liability have been suggested. As an example, the U.S. Department of Justice (DOJ) has argued that competitors' joint use of common pricing algorithms that rely on competitively sensitive nonpublic information to set prices can constitute concerted action and violate the Sherman Antitrust Act. However, there are few court decisions in this area, which makes it difficult to give a definitive answer as to whether any particular product would be free of antitrust risk.

When a group of competitors knowingly use the same algorithmic price comparison software and that software

relies on competitively sensitive nonpublic data, there is a greater risk of potential antitrust harms. The DOJ has filed suit against a software company alleging the use of such software is an unlawful scheme to decrease competition among landlords in apartment pricing and to monopolize the market for commercial revenue management software that landlords use to price apartments.

Courts have compared situations in which groups of competitors subcontract their pricing decisions to a common outside agent that provides algorithmic pricing services to a traditional hub-and-spoke price-fixing conspiracy, even if the competitors do not communicate with one another about the results of the algorithmic pricing. This is because the same outside vendor has confidential price strategy information and can program the algorithm to maximize industrywide pricing even if the individual competitors themselves do not directly share their competitively sensitive data.

In order to prevent potential antitrust issues resulting from the use of algorithmic pricing tools, businesses should consider the following practices:

- Do not automatically follow the tool's pricing recommendations; leave final decision-making authority to a human who will review the tool's recommendations and document such review.
- Do not discuss the algorithmic pricing tool with competitors. In lawsuits, plaintiffs have cited discussions among competitors at industry conferences, webinars and meetings hosted by software sellers as circumstantial evidence of a conspiracy.
- Continue to ensure that the tool relies on only public pricing data and that the output is aggregated pricing data and not suggested pricing.
- Be ready to reevaluate use of the tool if you become aware that it is being used by your competitors.
- Document the procompetitive benefits and results of using the tool, including lowered prices for consumers or increasing sales to meet increased consumer demand.
- When in doubt, seek advice from antitrust counsel.

Heightened Enforcement

In recent years, both private plaintiffs and the government have increasingly scrutinized businesses' use of algorithmic pricing software, leading to a wave of antitrust lawsuits and enforcement actions. Algorithmic collusion claims are still relatively new, and courts have not yet settled on clear legal standards to govern these claims. Regulatory scrutiny of algorithmic pricing tools that use competitor data, especially nonpublic information, has increased amid concerns about potential collusion. Federal agencies like the DOJ and Federal Trade Commission are investigating potential violations of antitrust and other laws. One area of particular attention is landlords sharing sensitive data for rental price-fixing.

How Does This Impact Businesses?

Even if they do not use personal, nonpublic or competitively sensitive data for determining their pricing, businesses using algorithmic pricing software should consistently evaluate their usage of pricing tools. It is crucial to ensure that independent decision-making remains central to pricing strategies to prevent unintended antitrust issues, remain compliant with all applicable laws and regulations and ensure that businesses respect and do not infringe upon individuals' privacy rights.

Related Professional

Sarah Rubenstein Polak . . . . . spolak@loeb.com