

Weighing the Cost: Retailers' Technology and Data Use When Setting Prices Subject to Increased Scrutiny

March 27, 2026

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

Executive Summary

- **What's new:** Algorithmic and “surveillance” pricing have increasingly become the target of litigation, legislation and regulatory investigations as consumers and policymakers continue to focus on affordability.
- **Why it matters:** Companies' algorithmic and surveillance pricing practices present increased legal risk in the rapidly shifting technological, legal and compliance landscape.
- **What to do next:** Retailers should evaluate the software and data they use to set prices, confirm compliance with recently enacted statutes, and monitor legislative and regulatory developments at the federal, state and local levels, as well as any related case law.

Retailers are increasingly deploying technology to make better-informed pricing decisions. This technology, such as pricing algorithms and other artificial intelligence tools, can help retailers more effectively use the vast quantity of proprietary, competitor and customer data they can access through, for example, dynamic prices tailored to supply and demand trends, prices personalized to a particular customer (a practice sometimes called “surveillance pricing”), or customer-specific coupons or rewards programs. Some of these technologies may rely on customers' personal data (including location, browser history, purchasing history and demographics) to set, recommend or adjust personalized prices. Others may rely on a retailer's proprietary pricing data or pricing data of competitors. While this use of data can create efficiencies and enhance competition by matching customers with products and offering lower prices, algorithmic and surveillance pricing is drawing scrutiny from private plaintiffs, legislators and regulators. Below, we discuss recent trends concerning both the use of the same algorithm by multiple competitors and companies' proprietary uses of data to personalize pricing.

Antitrust Litigation Involving Pricing Algorithms

The antitrust plaintiffs' bar and federal and state regulators have recently targeted the use of commercially available, third-party pricing algorithms by multiple competitors.

Pricing algorithms can generate pricing recommendations or automatically adjust pricing based on the analysis of data regarding customer behavior and market conditions. Although these tools often consider the same kinds of information that businesses have always relied on to inform their pricing decisions, pricing algorithms are able to process much higher volumes of data at significantly greater speeds than human analysts can. As a result, algorithmic pricing can respond more quickly to, and calculate based on a more accurate understanding of, real-time market conditions.

While companies frequently use pricing algorithms because of the efficiencies algorithms can yield, this practice has recently drawn a high level of scrutiny — and a high volume of litigation — from antitrust plaintiffs' lawyers and regulators. This trend began in October 2022, when public reporting on landlords' use of RealPage pricing algorithms to help price apartments in multifamily rental housing led to the filing of the first putative class-action complaint alleging an antitrust conspiracy based on the use

Weighing the Cost: Retailers' Technology and Data Use When Setting Prices Subject to Increased Scrutiny

of a common third-party pricing algorithm. Over 40 follow-on complaints alleging similar claims were ultimately consolidated in the Middle District of Tennessee. Similar lawsuits have since been filed alleging price-fixing via the use of other third-party pricing algorithms in multifamily housing, casino-hotels, luxury hotels and out-of-network health-care reimbursement, among other sectors. Plaintiffs in these cases have typically based their allegations on algorithm providers' publicly available marketing materials, which often include representative client lists or testimonials. If marketing materials show that multiple companies in an industry subscribe to pricing algorithms provided by the same third party, plaintiffs have alleged an antitrust conspiracy among the subscribers to fix prices through use of a common algorithm.

Government regulators have also scrutinized the use of pricing algorithms, including by filing their own lawsuits targeting algorithmic pricing. The Department of Justice (DOJ) and several state attorneys general sued RealPage and property managers in the United States District Court for the Middle District of North Carolina. Attorneys general in Arizona, the District of Columbia, Kentucky, Maryland, New Jersey and Washington have brought individual lawsuits in their respective jurisdictions. In addition, the DOJ and the Federal Trade Commission (FTC) filed statements of interest in private litigation involving multifamily rental housing, casino-hotels and out-of-network health-care reimbursement. In these statements of interest, the agencies have advanced an aggressive theory of algorithmic collusion, arguing that an antitrust conspiracy can be inferred from competitors' subscription to the same commercially available third-party algorithm, even if subscribers are not required to accept the algorithm's recommendations and even if each subscriber licensed the algorithm at different times.

Results

So far, the recent spate of algorithmic pricing litigation has yielded mixed results for plaintiffs. Several courts considering these complaints have dismissed them for failure to state a claim, and in the only published appellate decision so far, the U.S. Court of Appeals for the Ninth Circuit affirmed such a dismissal in litigation involving the use of pricing algorithms marketed by Cendyn Group to casino-hotels in Las Vegas. In that case, captioned *Gibson v. Cendyn Group*, the plaintiffs attempted to plead both a horizontal conspiracy among the software users as well as a challenge to each individual hotel's license with the software vendor. After the plaintiffs abandoned their horizontal conspiracy claim on appeal, the Ninth Circuit affirmed dismissal of the remaining claim, holding that a software license that allows subscribers to receive nonbinding pricing recommendations is not a "restraint of trade" — particularly where those recommendations do not rely on competitively sensitive information from a subscriber's rivals.

On the other hand, several algorithmic-pricing antitrust complaints have survived motions to dismiss and proceeded to discovery, including the RealPage multifamily rental housing litigation. Courts that have denied motions to dismiss have typically focused on allegations that the software in question commingles the competitively sensitive information of individual subscribers through a "give to get" model and generates pricing recommendations based on that nonpublic competitor data. Though many of the algorithmic pricing cases that have reached discovery remain pending, in one notable case in California state court, defendants prevailed at summary judgment where the evidence showed that the algorithm in question did not commingle nonpublic competitor data to form its suggestions. In other instances, including the RealPage litigation, cases that have survived motions to dismiss have resulted in settlements by some defendants involving commitments to alter their pricing practices and to pay, in some cases, millions of dollars to class plaintiffs and state attorneys general.

Emerging Risk Points

The developing case law suggests that retailers should review their own use of any third-party software tools in their pricing decisions. To the extent that these tools may be used by multiple competing retailers, commingle data about customers from multiple subscribers or provide incentives to accept pricing recommendations, retailers should seek advice from counsel about mitigating the risk of any potential antitrust claims.

Legal Challenges and Restrictions Related to Surveillance Pricing on the Horizon

Heightened scrutiny of personalized or "surveillance" pricing has followed in the wake of the algorithmic pricing cases, spurred by an increased policy focus on affordability. Personalized or surveillance pricing refers to retailers gathering customer data to create individualized profiles that may be used to assign different prices to different customers for the same product. This data can include geolocation, browsing and purchase history, demographics and technical specifications for online purchasers such as device type, battery life and mouse clicks.

Use of surveillance pricing can raise data privacy, transparency, discrimination, consumer protection and antitrust concerns. While consumer privacy statutes and proposed legislation limiting the use of surveillance pricing in many states include carve-outs for loyalty rewards or customer club cards, to the extent this data supplies an input into algorithmic pricing software that commingles competitor data, the data's use could present a risk of antitrust litigation, as discussed above.

Weighing the Cost: Retailers' Technology and Data Use When Setting Prices Subject to Increased Scrutiny

Surveillance pricing has drawn attention from the FTC. Between July 2024 and January 2025, the FTC conducted a surveillance pricing study pursuant to its authority under Section 6(b) of the FTC Act. In January 2025, the FTC released a research summary that described the increasingly “multi-dimensional” nature of prices and explained that through the use of surveillance pricing tools, “the same good may have different prices in different places or for different people or audience segments based on data gathered and used from various sources.” Respondents to the study included large companies such as Mastercard. The research summary reported that multiple respondents described their surveillance pricing tools as supporting revenue growth between 2-5%. The 6(b) study effectively ended after FTC leadership changed in 2025, but FTC officials, state regulators and legislators have demonstrated continued interest in surveillance pricing.

Recent Federal, State and Local Enforcement and Legislation

Legislation Targeting Algorithmic and Surveillance Pricing

Algorithmic and surveillance pricing, and their use in particular industries, have become the targets of a wave of newly enacted and proposed legislation at the federal, state and local levels.

Algorithmic Pricing Legislation

The additions of Cal. Business and Professions Code Sections 16729 and 16756.1 under California Assembly Bill 325 went into effect on January 1, 2026, and prohibit the use or distribution of “common pricing algorithms” in anticompetitive agreements. The new rules also prohibit the use or distribution of a common pricing algorithm where a person coerces another person to set or adopt a recommended price or commercial term.

Gov. Kathy Hochul signed New York Senate Bill 7882, New York General Business Law Section 340-b, which prohibits the use of software that makes price recommendations based on data other than the user’s own in the rental housing industry. RealPage is challenging the statute on First Amendment grounds.

Other states and municipalities that have passed legislation restricting the use of algorithmic pricing in rental housing include, among others, Connecticut, San Francisco, Philadelphia, Minneapolis, Seattle and Portland, Ore. Meanwhile, broad algorithmic pricing bans and bills focused on rental housing are currently pending in several states.

At the federal level, Sen. Amy Klobuchar introduced the Preventing Algorithmic Collusion Act of 2025, which would presume an agreement under federal antitrust law when companies share competitively sensitive information through a pricing algorithm. This bill has been referred to the Senate Judiciary Committee.

Surveillance Pricing Legislation

New York is the first state to enact a law related to the use of consumer data in pricing. The Algorithmic Pricing Disclosure Act requires retailers that set prices using an algorithm based on consumers’ personal data to display a disclosure stating, “THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA.” Personal data is defined as “any data that identifies or could reasonably be linked, directly or indirectly, with a specific consumer or device.” Failure to comply may result in civil penalties of up to \$1,000 per violation. A similar transparency bill is pending in Illinois.

Companion New York Senate and Assembly bills, S8623 and A9349, which are currently in committee, seek further restrictions and would prohibit the use of personalized algorithmic pricing that relies on personal data that “identifies or could be reasonably linked, directly or indirectly, with a specific consumer or device.” These bills also propose a disclosure requirement for entities that use software and algorithms to adjust the prices of goods and services based on factors other than consumers’ personal data. S8616 and A9396 propose similar bans on personalized algorithmic pricing by grocery and drug stores.

Legislators in several other states — including Arizona, Colorado, Florida, Hawaii, Nebraska, New Jersey, Tennessee and Washington — have proposed broad bans on surveillance pricing. At the federal level, Rep. Greg Casar introduced the Stop AI Price Gouging and Wage Fixing Act of 2025, which seeks to ban surveillance pricing and was referred to the House Committee on Energy and Commerce, the House Judiciary Committee and the House Committee on Education and Workforce. Also, Sens. Ruben Gallego, Kirsten Gillibrand, Cory Booker and Angela Alsobrooks introduced the One Fair Price Act of 2025 that would ban surveillance pricing. This bill was referred to the Senate Committee on Commerce, Science, and Transportation.

Maryland, New Jersey and Pennsylvania have also introduced bills specifically targeting grocery stores’ use of surveillance pricing. And House legislators have introduced the Stop Price Gouging in Grocery Stores Act, which was referred to the House Committee on Energy and Commerce and the House Judiciary Committee.

Weighing the Cost: Retailers' Technology and Data Use When Setting Prices Subject to Increased Scrutiny

Federal and State Inquiries Into Company Practices

Federal and state inquiries into e-commerce grocery delivery platform Instacart's pricing practices and data use highlight the increased government scrutiny of both algorithmic and surveillance pricing. In December 2025, *Consumer Reports* published a study that found that certain retailers' prices for groceries sold on Instacart "differed by as much as 23 percent per item from one Instacart customer to the next." Shortly thereafter, *Reuters* reported that the FTC sent Instacart a civil investigative demand related to the company's algorithmic pricing software.

On March 5, 2026, the House Committee on Oversight and Government Reform sent Instacart a letter inquiring about the company's surveillance pricing practices and the algorithmic pricing software the company offers to other retailers. The committee's letter notes that "deployment of algorithmic tools marketed to consumer-facing companies ensures that prices are coordinated[,] which could amount to implicit collusion to raise prices overall and may warrant further scrutiny under" federal antitrust law.

New York Attorney General Letitia James also sent a letter to Instacart requesting information about reports of substantial price variations among shoppers and suggesting that the company's pricing practices may have violated New York's algorithmic pricing disclosure law discussed above. And recently, California Attorney General Rob Bonta also sent letters to businesses with a significant online presence in the retail, grocery and hotel sectors as part of an investigation into whether surveillance pricing practices violate the California Consumer Privacy Act.

Next Steps

Retailers that use algorithmic or personalized pricing should assess their pricing practices and comply with any relevant disclosure requirements.

As the legal and legislative landscape evolves across jurisdictions, companies that use algorithmic or personalized pricing should evaluate their pricing practices and monitor new requirements, enforcement actions and developing case law related to the use of pricing algorithms and surveillance pricing.

Contacts

Boris Bershteyn

Partner / New York
212.735.3834
boris.bershteyn@skadden.com

Michael H. Menitove

Partner / New York
212.735.3517
michael.menitove@skadden.com

Adam G. Kochman

Associate / New York
212.735.2589
adam.kochman@skadden.com

Karen M. Lent

Partner / New York
212.735.3276
karen.lent@skadden.com

Anna E. Drootin

Associate / New York
212.735.3532
anna.drootin@skadden.com

Thomas (T.J.) Smith

Associate / New York
212.735.3829
thomas.smith@skadden.com