

AN A.S. PRATT PUBLICATION
SEPTEMBER 2026
VOL. 12 NO. 7

PRATT'S
**PRIVACY &
CYBERSECURITY
LAW**
REPORT



LexisNexis

EDITOR'S NOTE: THE NEXT FRONTIER

Victoria Prussen Spears

**SURVEILLANCE PRICING: THE NEXT
FRONTIER OF PRIVACY LITIGATION**

Matthew M. Morrissey, Josh Mahoney,
Michael William Fires, Kate C. Goldberg and
Tyler J. Hoguet

**DRIFT PROTOCOL EXPLOIT: WHY "SOCIAL
TRUST" IS THE NEWEST CYBERSECURITY GAP**

Rajeev Raghavan, Anand Sithian and
Sarah Rippy

**GENETIC DATA AND ARTIFICIAL INTELLIGENCE
TRAINING FOLLOWING ACQUISITIONS: EMERGING
LITIGATION RISK AND A RAPIDLY EXPANDING
STATE REGULATORY LANDSCAPE**

Jason Johnson, Linda Malek and Sarah Rippy

**NAVIGATING AI COMPLIANCE WITH HIPAA
ESSENTIALS**

Jeff Wurzburg, Susana Medeiros, Susan Linda
Ross, Abel Chacko and Kathleen Rubinstein

**THIRD CIRCUIT OFFERS CLARITY ON DATA
PRIVACY AND REPLAY CODE: 3 PROACTIVE
STEPS FOR BUSINESSES FOLLOWING
DUAL RULINGS**

Risa B. Boerner, Logan S. Booth and
Catherine M. Contino

**U.S. STATE PRIVACY ENFORCEMENT: KEY
PRIORITIES AND PRACTICAL GUIDANCE
FROM STATE REGULATORS**

Jason Johnson and Linda Malek

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12

NUMBER 7

September 2026

Editor's Note: The Next Frontier Victoria Prussen Spears	221
Surveillance Pricing: The Next Frontier of Privacy Litigation Matthew M. Morrissey, Josh Mahoney, Michael William Fires, Kate C. Goldberg and Tyler J. Hoguet	223
Drift Protocol Exploit: Why "Social Trust" Is the Newest Cybersecurity Gap Rajeev Raghavan, Anand Sithian and Sarah Rippy	236
Genetic Data and Artificial Intelligence Training Following Acquisitions: Emerging Litigation Risk and a Rapidly Expanding State Regulatory Landscape Jason Johnson, Linda Malek and Sarah Rippy	240
Navigating AI Compliance With HIPAA Essentials Jeff Wurzburg, Susana Medeiros, Susan Linda Ross, Abel Chacko and Kathleen Rubinstein	243
Third Circuit Offers Clarity on Data Privacy and Replay Code: 3 Proactive Steps for Businesses Following Dual Rulings Risa B. Boerner, Logan S. Booth and Catherine M. Contino	248
U.S. State Privacy Enforcement: Key Priorities and Practical Guidance From State Regulators Jason Johnson and Linda Malek	251

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at (908) 673-3380
Email: Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:
Customer Services Department at (800) 833-9844
Outside the United States and Canada, please call (518) 487-3385
Fax Number (800) 828-8341
LexisNexis® Support Center <https://supportcenter.lexisnexis.com/app/home>
For information on other Matthew Bender publications, please call
Your account manager or (800) 223-1940
Outside the United States and Canada, please call (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [article title], [vol. no.] PRATT’S PRIVACY & CYBERSECURITY LAW REPORT [page number]
(LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT’S PRIVACY &
CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2026 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW  BENDER

(2026–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES

Partner, Venable LLP

CHRISTOPHER G. CWALINA

Partner, Norton Rose Fulbright US LLP

RICHARD D. HARRIS

Partner, Day Pitney LLP

JAY D. KENISBERG

Senior Counsel, Rivkin Radler LLP

DAVID C. LASHWAY

Partner, Sidley Austin LLP

CRAIG A. NEWMAN

Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL

Partner, Sidley Austin LLP

RANDI SINGER

Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI

Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE

Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH

Partner, Thompson Hine

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2026 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Surveillance Pricing: The Next Frontier of Privacy Litigation

*By Matthew M. Morrissey, Josh Mahoney, Michael William Fires, Kate C. Goldberg and Tyler J. Hoguet**

In this article, the authors explain that companies should evaluate their current “surveillance pricing” practices to assess their exposure to enforcement activity and class action litigation.

Companies in a wide range of industries are finding creative new ways to collect and harness consumer data to deploy targeted or personalized pricing. However, these pricing strategies, which are commonly referred to as “surveillance pricing” or “algorithmic pricing,” are under heightened scrutiny from regulators, legislators, and law enforcement officials. Moreover, the evolving legal landscape regarding these practices may spark a new wave of class actions from the plaintiffs’ bar.

The increased focus on surveillance pricing began in July of 2024 when the Federal Trade Commission (FTC or Commission) launched a Section 6(b) investigative study into such practices. In January of 2025, the FTC published a preliminary “Research Summary” regarding the issue but took no further action. Since that time, federal enforcement activity has been relatively light. Nonetheless, California Attorney General Rob Bonta launched an investigation regarding these issues in January of 2026. New York Attorney General Letitia James has also issued a consumer alert on “surveillance pricing,” and she recently launched an investigation into a prominent consumer-facing company’s surveillance pricing disclosures.

On the legislative front, two federal laws that address surveillance pricing issues have been proposed but have not yet been signed into law. The state legislative landscape is rapidly changing. In April of 2026, Maryland passed the first law in the country to ban surveillance pricing in certain industries. The Maryland law precludes the use of surveillance pricing for certain food retailers and third-party delivery service providers. Since December of 2025, New York has required specific disclosures regarding surveillance pricing, but the New York law does not ban the practice. The Maryland and New York laws do not include a private right of action. Over 20 other state legislatures have now introduced legislation that seeks to regulate or ban surveillance pricing outright for at least some industries. A number of these statutes grant consumers a private right of action, include statutory damages provisions, and allow for the recovery of attorneys’ fees.

* The authors, attorneys with Faegre Drinker Biddle & Reath LLP, may be contacted at matthew.morrissey@faegredrinker.com, josh.mahoney@faegredrinker.com, michael.fires@faegredrinker.com, kate.goldberg@faegredrinker.com and tyler.hoguet@faegredrinker.com, respectively.

If passed, the proposed federal and state statutes could lead to a significant wave of class action litigation. The plaintiffs' bar may also attempt to assert claims for violations of federal and state privacy statutes, state consumer fraud statutes, and other common law theories of liability. As perhaps a harbinger of future trends, plaintiffs have filed two of the first putative class actions regarding surveillance pricing against JetBlue Airlines in the Eastern District of New York.¹ The plaintiffs' bar has also challenged surveillance or algorithmic pricing strategies under federal and state antitrust laws. Although many of these antitrust claims have failed due to plaintiffs' inability to prove that defendants shared consumer pricing data, other cases have survived dismissal, and one case recently resulted in a significant settlement.

The following sections of this article provide additional information regarding the multifaceted scrutiny of surveillance pricing strategies. Additionally, this article provides strategic considerations and recommendations to help companies assess their exposure to enforcement activity or class action litigation claims.

WHAT IS PERSONALIZED OR "SURVEILLANCE" PRICING?

It is important to distinguish between "surveillance" or "algorithmic" pricing and other forms of supply-and-demand-based dynamic pricing. Certain industries use dynamic pricing models to adjust prices in response to real-time supply and demand. For example, the price of an airline ticket may increase as a plane approaches passenger capacity, or it may decrease if numerous seats remain empty. While these practices may result in consumers paying different prices for the same goods or services, they have not been the focus of increased scrutiny.

"Surveillance pricing" refers to a company setting prices for individual consumers based on attributes unique to the individual consumers that are unrelated to broader supply or demand pressures. According to the FTC,² surveillance pricing involves using "advanced algorithms, artificial intelligence and other technologies with personal information about consumers . . . to categorize individuals and set a targeted price for a product or service." Specifically, a company may charge otherwise similarly situated consumers different prices based on personal data that a company either purchases from third parties or aggregates on its own with respect to that customer. What differentiates "surveillance" pricing from other dynamic pricing practices under the FTC's definition is the use of *personal* data to set prices for individual consumers.

¹ See *Phillips v. JetBlue Airways Corp.*, No 1:26-cv-02405 (E.D.N.Y. Filed April 22, 2026); *Squire v. JetBlue Airways Corp.*, No. 1:26-cv-02629 (E.D.N.Y. Filed May 1, 2026).

² https://www.ftc.gov/system/files?file=ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf.

FEDERAL & STATE ENFORCEMENT ACTIVITY

The FTC's Initial Investigation & Research Summary

In response to media reports and growing consumer interest, the Federal Trade Commission initiated a study of surveillance pricing using its Section 6(b) investigative authority in July of 2024. The FTC's inquiry focused on several third-party intermediaries that offer pricing products to retailers. The pricing products at issue analyze consumers' personal information using artificial intelligence, algorithms, and other advanced technologies to set prices for goods or services. The FTC asked these companies to provide information concerning their product offerings, data collection methods, and customer and sales information to determine whether and to what extent surveillance pricing impacts consumers and prices.

In January 2025, the Commission took the unusual step of publishing³ a preliminary "Research Summary" of its findings to date rather than complete Section 6(b) studies and reports. As detailed in the Summary, the Commission found evidence that companies were using consumers' data — including their location, browsing history, and demographic traits — to charge consumers different prices for the same goods. The Summary also described some of the ways in which retailers were already using the tools and services it studied:

For instance, if a consumer is profiled as a new parent, the consumer may intentionally be shown higher priced baby thermometers on the first page of their in-app search results, based on their residential zip code and time of purchase. These tools could also potentially be used to collect behavioral details that a retailer could use to forecast a customer's state of mind, like using a shopper's selection of "fast-delivery" shipping on an order of infant formula to infer that a shopper could be a rushed parent who may be less price-sensitive.

The comment period for the FTC study closed on January 24, 2025, and the Commission has not engaged in further studies or rulemaking related to surveillance pricing since the publication of the Summary. In December of 2025, however, the FTC issued a Civil Investigative Demand to a delivery service company seeking information on its use of an AI tool to inform its pricing. The Demand indicates the potential for renewed interest from the current administration.

Other Federal Enforcement Activity

On March 5, 2026, the Chairman of the House Committee on Oversight and Government Reform (the Committee) also launched an investigation into the use of AI in surveillance pricing. The Committee sent letters to several consumer-facing companies requesting similar information across each respective industry about AI-based pricing,

³ https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf.

the use of consumer data, third-party data sources, pricing experiments, and disclosures to consumers. The Committee's letters noted that companies use personal data to "determine a consumer's emotional state, purchase intent, [and] maximum willingness to pay" to tailor an individualized price, but consumers rarely have insight into "what information a company has about them, what the prices they see are based on, or what prices other customers may be seeing for the same goods or services — making it difficult for consumers to make informed purchasing decisions." The Committee cites the FTC report and consumer watchdog reports, as well as both the *Wall Street Journal* and *Jacobin*, indicating skepticism across the political spectrum.

State Enforcement Activity

In addition to the House Committee's investigation, states are also beginning to take action. On January 27, 2026, California Attorney General Rob Bonta announced an investigative sweep targeting surveillance pricing practices by sending inquiry letters to prominent businesses in the retail, grocery, and hotel sectors. The inquiry requests information about how these companies use consumers' personal information, including shopping and browsing histories, locations, demographics, and other data, to set individualized prices. The inquiry also requests information on these companies' policies, public disclosures, and compliance with privacy and competition laws. Attorney General Bonta intends to use the California Consumer Privacy Act's (CCPA) "purpose limitation" to limit how companies use personal information in ways that are consistent with the "reasonable expectations" of consumers.

THE EVOLVING LEGAL LANDSCAPE

Proposed Federal Legislation

The Stop AI Price Gouging and Wage Fixing Act, H.R. 4640,⁴ and the Stop Price Gouging in Grocery Stores Act, H.R. 4966,⁵ propose significant federal restrictions on the use of surveillance and dynamic pricing technologies in retail grocery stores and in setting wages.

Under the Stop AI Price Gouging and Wage Fixing Act, individuals, partnerships, corporations, and other entities would not be allowed to engage in "surveillance-based price setting" based on personal information, genetic information, behavior, or biometrics of an individual or of a group. These entities would also have to disclose any processes and policies associated with automated decision-making systems that determine pricing. However, discounts applied uniformly based on occupation, age, military service, student status, or participation in reward programs would still be allowed. Additionally, entities would not be allowed to engage in "surveillance-based wage setting," defined as the use of automated technology to consider personal information or surveillance data

⁴ <https://www.congress.gov/bill/119th-congress/house-bill/4640>.

⁵ <https://www.congress.gov/bill/119th-congress/house-bill/4966>.

to set or inform how an individual is compensated. This would include hourly rates, salaries, bonuses, commissions and other incentives, scheduling, task management, and other material terms that would have a direct impact on a worker's earnings. However, entities would still be allowed to consider the city or state and the cost of living.

Under the Stop Price Gouging in Grocery Stores Act, retail grocery stores would be prohibited from selling items at enhanced prices and from adjusting the price of an item for a consumer based on personal information, including through the use of facial recognition or the use of electronic shelf labels. The legislation would specifically ban stores over 10,000 square feet from using electronic shelf labels and would require these larger retailers to present prices using nondigital displays. However, discounts applied uniformly based on occupation, age, military service, student status, or participation in reward programs would still be allowed. Any use of biometric data by retail grocery stores would only be permitted with the informed consent of the consumer.

The enforcement mechanisms under these acts would grant enforcement authority to the FTC, state attorneys general, and private individuals. The Equal Employment Opportunity Commission (EEOC) would also be able to enforce violations regarding surveillance-based wage setting. Consumers would have a private right of action allowing them to seek \$3,000 in statutory damages, actual monetary damages, or injunctive relief for violations, with willful and knowing violations subject to treble damages. Lastly, under both laws, courts would be able to award prevailing plaintiffs any costs and reasonable attorneys' fees. Both bills have since been referred to committee.

Twenty-eight representatives have also expressed support for the Federal AI Civil Rights Act, H.R. 6356,⁶ which would prohibit both developers and deployers from offering, licensing, promoting, selling, or using covered algorithms in ways that would cause disparate impact or otherwise discriminate against individuals, or make the equal enjoyment of goods, services, activities, or opportunities unavailable. This legislation would apply to any algorithm that could affect access to these offerings and would specifically target potential discrimination resulting from the use of AI.

The legislation would mandate a series of assessments and reporting requirements for developers and deployers. Before deploying any covered algorithm, developers and deployers would be required to conduct a plausibility assessment to evaluate whether the algorithm could result in harm, followed by an independent pre-deployment audit. Additionally, developers and deployers would be obligated to conduct annual reviews of each impact assessment and regularly report findings to the commission. As with the bills above, the enforcement mechanisms under the act would grant authority to the FTC, state attorneys general, and private individuals to seek treble damages or \$15,000 per violation, whichever is greater. Lastly, courts would be able to award prevailing plaintiffs any costs and reasonable attorneys' fees.

⁶ <https://www.congress.gov/bill/119th-congress/house-bill/6356>.

EXISTING STATE LAWS

Maryland: Protection from Predatory Pricing Act

On April 28, 2026, Governor Wes Moore signed the Protection from Predatory Pricing Act, making Maryland the first state in the country⁷ to ban the use of surveillance data to increase prices in certain industries. Under the new law, food retailers in stores over 15,000 square feet and third-party delivery service providers may not use dynamic pricing or personal data to set a higher price for food already exempt from the state sales and use tax, which includes staple goods such as produce, bakery items, dairy products, and meats. Additionally, food retailers and delivery service providers may not use protected class data to offer, advertise, or sell goods or services in such a way that would result in denying accommodations, advantages, or privileges otherwise available. However, the law does not include a private right of action. Instead, the law requires the Attorney General or Division of Consumer Protection to provide the retailer with a 45-day opportunity to cure a violation before being subject to enforcement under the Maryland Consumer Protection Act, which provides for a \$10,000 penalty for the first offense and up to \$25,000 for subsequent offenses.

New York: GBL 349-a

On December 19, 2025, New York enacted the Fostering Affordability and Integrity through Reasonable (FAIR) Business Practices Act — the first legislation in the United States to address surveillance pricing. N.Y. Gen. Bus. Law § 349-a. Rather than banning the practice, GBL § 349-a requires any entity using “personalized algorithmic pricing,” defined as dynamic pricing set by an algorithm using data that identifies or could reasonably be linked with a specific consumer or device, to include a clear and conspicuous disclosure at the point of sale stating: “THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA.”

There is no private of right action under Section 349-a. Before the New York Attorney General may pursue an enforcement action, it must issue a cease-and-desist letter specifying the alleged violations. If the violations continue, the statute authorizes the Attorney General to pursue injunctive relief and civil penalties of up to \$1,000 per violation.

On January 8, 2026, the New York Attorney General's Office issued a letter to a food delivery company stating that it was investigating whether the company's notice provision at its point of sale complied with the statute. The letter cautioned that the use of “fine print text” may not comply with the Act's requirements that the disclosures be “clear and conspicuous.”

⁷ <https://governor.maryland.gov/news/press-releases/governor-moore-signs-legislation-protect-marylanders-pocketbooks-grocery-stores-safeguard-voting>.

California Consumer Privacy Act Enforcement

In the future, private plaintiffs or California enforcement authorities may allege that surveillance pricing violates state consumer privacy statutes, particularly the California Consumer Privacy Act (CCPA). The CCPA's "purpose limitation principle" prohibits regulated businesses from using a consumer's personal information in a manner inconsistent with a consumer's reasonable expectations.⁸ The CCPA's implementing regulations further require that businesses identify "the specific business or commercial purpose for collecting personal information from consumers" in a manner that "provides consumers a meaningful understanding of why the information is collected."⁹ When information is shared with third parties, businesses must describe in "specific" terms the purpose for which the data is collected.¹⁰

At the time of writing, no private suits have been filed seeking recovery under the theory that surveillance pricing violates the CCPA's "purpose limitation principle." Nonetheless, as discussed above, California Attorney General Rob Bonta has signaled that companies using surveillance pricing may violate the "purpose limitation principle" if they use consumer data to establish or alter prices "without proper disclosure." Collecting consumer information for the purpose of setting or altering prices without appropriate disclosures, and transmitting that data to third parties to assist with pricing strategies, may significantly increase a company's exposure to CCPA claims.

PROPOSED STATE LEGISLATION & FUTURE RISKS

Due to increased media coverage and interest from the FTC, over 20 state legislatures have introduced legislation that addresses or bans surveillance pricing for at least some industries. While several bills, such as Illinois Senate Bill 2255 and California AB 2564, ban the use of surveillance pricing in all industries, other proposed statutes focus only on essential goods and services, such as groceries.

Notably, some of these statutes grant consumers a private right of action for violations of the statute. For example, New York State Assembly Bill A9349 would ban the use of surveillance pricing and authorize consumers to bring a cause of action for:

- (i) actual damages, including any overcharges or lost discounts;
- (ii) injunctive or declaratory relief; and
- (iii) statutory liquidated damages between \$550 and \$5,000 per violation.

Similarly, Illinois Senate Bill 2255 prohibits the use of "surveillance data as part of an automated decision system to inform the individualized price assessed to a consumer

⁸ Cal. Civ. Code § 1798.100(c).

⁹ Cal. Code Regs. tit. 11, § 7011(e)(1)(C).

¹⁰ Cal. Code Regs. tit. 11, § 7051(a)(2).

for goods or services.” Consumers injured under the Illinois law could bring suit seeking (i) actual damages sustained, or (ii) \$3,000 for each violation. Furthermore, under the proposed Illinois statute, a consumer could seek three times the amount of actual damages sustained if the defendant violated the statute intentionally or in bad faith. Florida’s proposed SB 1746 similarly would authorize plaintiffs to recover actual damages or civil penalties up to \$1,500 per violation.

All of these proposed laws that authorize private rights of action would make each time a consumer is charged a price set by an algorithm using personal information a *separate violation* for damages purposes. For example, under the New York statute, if a consumer ordered from an online retailer once a week for a year and was charged a price based on that consumer’s personal information on every occasion, that consumer could bring a suit seeking \$5,000 for each and every order. The proposed statutes would also permit a prevailing plaintiff to recover attorneys’ fees.

Some proposed legislation would indirectly provide consumers a private right of action by defining surveillance pricing as a deceptive or unfair trade practice. For example, Texas SB 2567 would amend the Texas Unfair and Deceptive Trade Practices Act to include, as a defined unfair practice, using artificial intelligence or algorithmic software to set prices without disclosing it to consumers. The Texas Deceptive Trade Practices Act permits a consumer to recover their actual economic damages and emotional damages for knowing violations of the Act. Other proposed legislation only allows for injunctive relief. California AB 2564, for example, authorizes a private right of action for individuals aggrieved by surveillance pricing, but a prevailing plaintiff may only seek injunctive relief, attorneys’ fees, and costs.

Ultimately, there is significant variation across the proposed legislation concerning whether a statute:

- (i) would ban the use of algorithmic entirely or only require the disclosure of its use;
- (ii) is industry specific or general; and/or
- (iii) authorizes a private right of action to pursue damages, civil penalties, and/or attorneys’ fees.

PRIVATE LITIGATION TRENDS

There have been a handful of recent private consumer lawsuits challenging algorithmic or dynamic pricing on antitrust grounds. Most of these cases involve allegations that competitors agreed to use a common pricing algorithm or AI-driven tool to coordinate

prices. In antitrust terms, this is typically framed as a “hub-and-spoke” conspiracy, where the pricing vendor serves as the “hub,” competing firms are the “spokes,” and the necessary “rim” of the conspiracy is either an express or implied agreement among those competitor firms to adhere to the pricing tool’s outputs.¹¹

By contrast, until recently, there have been few private lawsuits attacking “surveillance pricing” under the prevailing privacy laws or state consumer fraud theories of liability. That may be changing.

On April 22, 2026, a plaintiff filed suit against JetBlue Airways, alleging that JetBlue’s use of individualized consumer data — collected through website tracking technologies and shared with third-party analytics and pricing vendors — violates the federal Electronic Communications Privacy Act (ECPA), the New York Unfair and Deceptive Trade Practices Act, and the New York Unlawful Selling Practices Act. The plaintiff purports to represent a putative nationwide class as well as a New York subclass. The complaint characterizes the lawsuit as “one of the very first class actions in American history regarding dynamic surveillance pricing.”¹² The filing follows reporting of a now-deleted social media exchange in which JetBlue appeared to suggest that pricing could vary based on browser data. The complaint repackages those reports as allegations that JetBlue adjusts fares based on user-specific website data, including search behavior and session history.¹³

The complaint alleges that the data collected by airline carriers like JetBlue is inherently “highly sensitive,” including both personally identifiable information and detailed transaction-level data relating to a customer’s flight selection. The complaint contrasts JetBlue’s public representations — e.g., that its “privacy commitments are fundamental to the way we run our business” — with alleged omissions in its privacy policy and cookie disclosures. Specifically, JetBlue allegedly does not disclose its use of specific data inputs — such as “IP address,” “geo-location data,” “pages visited,” and “purchases and purchase history” — to inform pricing, or that it shares such data with third parties to develop pricing. Plaintiff alleges that JetBlue uses these data inputs to set fares based on individualized “buyer behavior” rather than market conditions alone.

The *Phillips v. JetBlue* case may spark a wave of surveillance-pricing-related class actions asserting claims under state and federal privacy laws, state consumer protection statutes, future surveillance pricing statutes, and other common law theories of liability.

¹¹ A discussion of antitrust cases involving algorithmic pricing conspiracies is outside the scope of this article. Examples of these types of cases include *In re RealPage, Inc., Rental Software Antitrust Litig.* (No. II), 709 F. Supp. 3d 478 (M.D. Tenn. 2023); *Gibson v. Cendyn Grp., LLC*, 148 F.4th 1069 (9th Cir. 2025); *Mach v. Yardi Systems, Inc.*, (Cal. Super. Aug. 19, 2024); *Duffy v. Yardi Sys., Inc.*, 758 F. Supp. 3d 1283 (W.D. Wash. 2024).

¹² *Phillips v. JetBlue Airways Corp.*, No. 1:26-cv-02405 (E.D.N.Y.).

¹³ It does not appear that the individual who interacted with JetBlue on social media is the named plaintiff in the lawsuit.

In fact, a Virginia-based plaintiff has filed a second lawsuit against JetBlue in the Eastern District of New York that raises nearly identical factual allegations.¹⁴ The *Squire* plaintiff seeks relief under the ECPA and the New York statutes at issue in *Phillips*, and also asserts claims under the Virginia Consumer Protection Act and the Virginia Wiretap and Eavesdropping Act. Moreover, the *Squire* plaintiff asserts these claims individually, as well as on behalf of a putative nationwide class and a Virginia consumer subclass.

The antitrust plaintiffs' bar will also be following the two JetBlue cases closely, as similar allegations could readily be repackaged into antitrust claims. For example, to state a monopolization claim under Section 2 of the Sherman Act, a plaintiff must allege (i) monopoly power in a properly defined relevant market, and (ii) exclusionary conduct. The former requires defining both a product and geographic market and plausibly alleging the ability to control prices or exclude competition, often through market share and barriers to entry. The latter requires conduct that harms competition, not merely competitors. While courts have made clear that vigorous competition — including price-cutting — is lawful, conduct such as predatory pricing can, in certain circumstances, constitute unlawful monopolization.¹⁵

Viewed in that light, surveillance pricing theories could gain traction — particularly where plaintiffs plausibly allege both market power and the use of data-driven pricing tools to distort competitive conditions. For example, plaintiffs may contend that such tools enable firms to target specific consumers or segments to foreclose rivals, or to selectively underprice competitors in the short term to gain market share before raising prices. At a minimum, these types of allegations — especially when coupled with detailed claims regarding data collection, third-party analytics, and real-time pricing — may be sufficient to survive a motion to dismiss, exposing companies to wide-ranging discovery into pricing strategies, systems, and methodology, along with scrutiny of companies' associated data practices.

In sum, while the JetBlue cases assert claims under privacy and consumer fraud statutes, they may ultimately be viewed as a harbinger of a broader wave of consumer class actions that challenge data-driven pricing practices not only under privacy laws, state consumer protection statutes, or future surveillance pricing statutes, but also under federal antitrust law, with the attendant risk of treble damages depending on the market context and the role of data in shaping individualized pricing.

STRATEGIC CONSIDERATIONS

Due to the heightened scrutiny of surveillance pricing practices and the evolving legal landscape, companies should assess their exposure to enforcement activity and class action litigation claims. As a part of this analysis, companies should consider the following issues:

¹⁴ *Squire v. JetBlue Airways Corp.*, No. 1:26-cv-02629 (E.D.N.Y.).

¹⁵ See *Brooke Group Ltd. v. Brown & Williamson Tobacco Corp.*, 509 U.S. 209 (1993).

Assess Current Practices

Companies should ensure that they understand their current practices regarding the collection, dissemination, and use of data from consumers, including:

- Is any data collected from consumers being used to establish or modify pricing?
- Does the company transmit consumer data to any third parties for any purpose, including but not limited to establishing or modifying pricing?
- Is the company using third parties to establish or modify pricing? If so, take proactive steps to understand how the third parties are generating the prices and whether they are utilizing any data from consumers in this process.

Analyze Compliance with Existing Laws

Companies should assess whether they are complying with the existing legal framework regarding surveillance pricing, including:

- Does the Maryland Protection from Predatory Pricing Act apply to the company?
- Is the company complying with the New York GBL Section 349-a disclosure requirements if it is using the pricing practices regulated under the statute?
- Is the company complying with the CCPA's "purpose limitation principle?"

Review Current Policies, Disclosures, & Consumer Consents

Companies should assess if their current privacy policies, terms of use, and other consumer disclosures accurately state how consumer data is being used, whether any such data is being transmitted to third parties, and whether any such data is being used to establish or modify pricing. Companies should also assess whether they are obtaining consent from consumers for their data practices, and whether the consents extend to the company's pricing strategies.

- Consider updating the company's policies, disclosures and consumer consents as needed to address any identifiable gaps.

High-Risk Industries

Based upon the current legislative and enforcement trends, companies operating in the following industries may have a heightened risk of claims related to surveillance pricing practices: aviation, grocery stores, big-box retailers, food and grocery delivery apps, hotel operators, and multifamily rental housing companies.

Monitor Developments Closely

The legal framework related to surveillance pricing is rapidly evolving. Companies utilizing pricing strategies that may come under scrutiny should ensure that they are actively monitoring all developments, including:

- Companies should analyze how the proposed federal and state legislation regarding surveillance pricing may impact their business if passed into law.

Other Considerations

Companies that are currently using pricing strategies that may come under heightened scrutiny or companies that are considering using such strategies should consider the following issues in addition to the ones highlighted above:

- Does the pricing practice impact the prices that consumers pay? If so, what is the scope of the pricing variations? How much has the company profited (if at all) from the use of the pricing practice?
- Does the pricing practice result in different prices in certain geographic areas or cities? Are the prices different on an individual level?
- Will the use of the pricing practices create differences between shelf pricing or advertised prices, and the prices consumers pay at check-out?
- Are the pricing practices used for either “brick and mortar” transactions or electronic transactions?
- Could the pricing practices be deemed to be confusing or misleading to a “reasonable” consumer?
- Could the pricing practices inadvertently create adverse pricing impacts for protected classes of individuals?

Understand that a court may consider the totality of the circumstances, including information concerning a retailer's size, history, controls, and profit opportunity, when evaluating a pricing practice.

IN SUMMARY

- Companies in a wide range of industries are finding creative new ways to collect and harness consumer data to deploy targeted or personalized pricing.
- However, these pricing strategies, which are commonly referred to as “surveillance pricing” or “algorithmic pricing,” are under heightened scrutiny from regulators, legislators, and law enforcement officials.

- Congress is considering several proposed laws that would impose significant restrictions or outright bans on “surveillance pricing.” Additionally, over 20 state legislatures have introduced legislation that seeks to regulate or ban surveillance pricing outright in at least some industries. A number of these statutes grant consumers a private right of action, include statutory damages provisions, and allow for the recovery of attorneys’ fees.
- The evolving legal landscape regarding these pricing strategies may spark a new wave of class action litigation from the plaintiffs’ bar. In fact, a major airline was recently named as a defendant in one of the first putative class actions ever filed alleging claims related to surveillance pricing practices. A separate plaintiff has already filed a second putative class action against the same airline based on virtually identical factual allegations and substantially similar legal theories.
- Companies should take immediate steps to assess their exposure to enforcement activity or class action litigation claims related to their pricing strategies.