When Pricing Gets Personal: Defining and Understanding Surveillance Pricing

David B. Hamilton, Emily W. Collins, and Caroline C. Olsen

Introduction

As artificial intelligence (AI) and machine learning programs become increasingly influential in the realm of consumer products or services, so-called "surveillance pricing" is moving from the fringes of academic debate to mainstream antitrust and consumer protection discussions. Key to these conversations is a clear understanding of what surveillance pricing is, and what it is not. Surveillance pricing refers to the use of consumer-specific data—often by intermediaries employing AI or machine learning—to set or steer individualized prices or promotions.[1]

Critically, surveillance pricing is distinct from algorithmic pricing writ large and dynamic pricing based on observable market conditions. While all three can involve automated systems, surveillance pricing uniquely relies on consumers' data trails.[2] Underpinning any discussion of surveillance pricing is the inherent perceived unfairness of the price discrimination that could result from surveillance pricing. That said, as discussed below, there are also procompetitive justifications for surveillance pricing. This Article surveys the current state of surveillance pricing in the United States, anchored in the Federal Trade Commission's (FTC) recent Section 6(b) study, emergent federal and state legislation, and existing legal tools under the Sherman Act, Robinson-Patman Act, and the FTC Act to help firms evaluate the legal risks when developing any pricing tools.

This Article proceeds as follows: Part I defines the core terminology—surveillance pricing, algorithmic pricing, and dynamic pricing—and explains why distinguishing among these practices is essential for legal analysis and compliance design. Part II turns to the FTC's ongoing Section 6(b) study, summarizing the scope of the agency's inquiry, its preliminary observations about data use and pricing tools, and the status of its work. Part III surveys emerging legislative and regulatory efforts at the federal, state, and international levels, highlighting disclosure mandates, proposed prohibitions, and the evolving debate over federal preemption. Part IV analyzes how existing U.S. legal frameworks—including antitrust law, Section 5 of the FTC Act, and privacy statutes—apply to surveillancepricing practices and where important gaps remain. Part V examines recent enforcement actions involving data flows and algorithmic tools, illustrating how current cases illuminate the infrastructure that enables individualized pricing. Part VI evaluates the economic literature on welfare and distributional effects, identifying the conditions under which personalized pricing may

■

David B. Hamilton *is a partner at DLA Piper.* ***Emily W. Collins*** *is of counsel, and* ***Caroline C. Olsen*** *is an associate at DLA Piper.*

[1] Fed. Trade Comm'n, *FTC Surveillance Pricing 6(b) Study: Research Summaries: A Staff Perspective* 1–2 (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf [hereinafter FTC 6(b) Study].

[2] Stephanie T. Nguyen & Samuel A.A. Levine, *Surveillance Pricing Update & The Work Ahead*, Fed. Trade Comm'n (Jan. 17, 2025), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2025/01/surveillance-pricing-update-work-ahead.

benefit or harm consumers. Finally, Part VII offers practitioner-focused governance guidance, outlining concrete steps firms can take to build compliant and auditable pricing systems.

I. Defining Terms: Surveillance, Algorithmic, and Dynamic Pricing

Surveillance, algorithmic, and dynamic pricing. These terms are often conflated in public debate, but precision is essential for legal analysis and compliance design.

"Algorithmic pricing" describes tool-enabled price setting, ranging from rules-based engines to AI-driven models.[3] Dynamic and surveillance pricing are essentially sub-types of algorithmic pricing, using algorithms to set prices. The key distinction is this: input. The information going into the algorithm is indicative of the pricing output.

"Dynamic pricing" uses market data, such as demand, inventories, or rival prices, to adjust prices in real-time or near-real-time.[4] It need not engage consumer-specific inputs. Airlines, for example, use dynamic pricing to determine the fare, relying on information like "seasonality, capacity, fuel costs, and other market metrics."[5] Using algorithms, dynamic pricing leverages this market data to quickly adjust prices, creating a "market-wide adjustment."[6] Thus, consumers buying at a particular moment in time all pay the same price. The price is not tailored to individual consumers; it is tailored to the current market.[7]

"Surveillance pricing," by contrast, uses individual personal or behavioral data, including location, browsing history, device signals, or purchase patterns. The output is individualized (or micro-segment) prices or tailored discounts and product rankings that alter the effective price paid.[8] Unlike dynamic pricing, surveillance pricing often results in consumers paying different prices, even when making the same purchase, at the same time.[9]

How do algorithmic pricing models access this personal and behavioral data? The FTC emphasizes that common online targeting mechanisms can be repurposed for pricing and steering.[10] Cookies and mobile software development kits (SDKs) that monitor ad responses can equally track reactions to product displays or discounts, enabling individualized promotions or rank-ordering of results.[11] Surveillance pricing models can then use this data to exclude "routine, regular customers" from promotions inferred to be unnecessary while sending targeted codes to "at risk" or infrequent buyers, or to reorder search results, presenting higher-priced options first for certain profiles.[12] As an illustration, it has been reported that certain hotel booking sites showed "substantially higher" prices to individuals browsing from more affluent cities than to individuals browsing

---

[3] Gabriella Antonie et al., *Personalized Pricing: Antitrust and Policy Considerations in the Age of Personalization*, 1 Antitrust Chron. 32, 33 (2025).

[4] John M. Yun, *Should We Fear Personalized Pricing?*, 1 Antitrust Chron. 8, 9–10 (2025).

[5] *Id.* at 9.

[6] *Id.*

[7] *See id.*

[8] *Id.*; Antonie et al., *supra* note 3, at 41.

[9] *See* Yun, *supra* note 4, at 9.

[10] FTC 6(b) Study, *supra* note 1, at 5–6.

[11] *Id.*

[12] *Id.* at 3–4.

from less affluent cities.[13] Such practices have captured the attention of the FTC, which seeks to map and assess surveillance pricing in greater detail.

II. The FTC's 6(b) Study: Scope, Early Observations, and Status

In July 2024, the FTC invoked Section 6(b) to order eight firms to produce information about "targeted pricing" and "user segmentation solutions," with an explicit focus on the third-party intermediaries that "enabl[e] firms to algorithmically tweak and target their prices."[14]

In January 2025, FTC staff published preliminary research summaries describing initial, non-exhaustive observations.[15] Staff reported that granular consumer data—such as precise location, browser history, and even mouse movements on a webpage—can be collected and leveraged to tailor prices and promotions for the same goods and services.[16] Staff also noted rank-ordering and recommendation tools that alter what consumers see, affecting effective prices even when a nominal list price is unchanged.[17]

FTC staff defined the scope of the inquiry to include cataloging products and services offered by third-party intermediaries; analyzing how their tools work to target prices or segment users; identifying the industries involved, data sources, and collection methods; and observing the effects on prices, sales, revenue, and consumers.[18] The summaries stress limitations, such as partial productions, aggregation/anonymization, and, generally, evolving insights while document review continues.[19] While the Commission briefly issued a public Request for Comment on January 17, 2025, the Commission withdrew the Request on January 22, 2025.[20] The study remains ongoing, the findings of which will be made public "time to time" when "disclosure . . . serve[s] the public interest."[21]

In addition to investigating surveillance pricing models that use consumer-data inputs, the FTC has also emphasized concerns about algorithmic pricing more generally.[22] Specifically, where algorithms ingest rivals' prices at a high frequency, there is a heightened risk of "soften[ed] price competition" even absent an agreement, a theme echoed in recent economic work.[23]

---

[13] *See, e.g.*, Keith A. Spencer, *Hotel Booking Sites Show Higher Prices To Travelers from Bay Area*, SFGATE (Feb. 3, 2025), https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php.

[14] Press Release, *FTC Issues Orders to Eight Companies Seeking Information on Surveillance Pricing*, Fed. Trade Comm'n (July 23, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-issues-orders-eight-companies-seeking-information-surveillance-pricing; FTC 6(b) Study, *supra* note 1, at 2.

[15] *See generally* FTC 6(b) Study, *supra* note 1, at 2.

[16] *Id.* at 2–6.

[17] *Id.* at 4–5.

[18] *Id.* at 5–10.

[19] *Id.* at 2–3.

[20] Nguyen & Levine, *supra* note 2; *Statement Regarding Request for Public Comment Re: Surveillance Pricing Practices*, Office of Commissioner Lina M. Khan (Jan. 31, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/khan-statement-regarding-request-for-public-comment-re-surveillance-pricing-practices.pdf.

[21] FTC 6(b) Study, *supra* note 1, at 2; Press Release, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices*, Fed. Trade Comm'n (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[22] *See, e.g.*, Press Release, *FTC and DOJ File Statement of Interest in Hotel Room Algorithmic Price-Fixing Case*, FTC (Mar. 28, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-doj-file-statement-interest-hotel-room-algorithmic-price-fixing-case.

[23] *See, e.g.*, Zach Y. Brown & Alexander MacKay, *Competition in Pricing Algorithms*, 15 Am. Econ. J.: Microeconomics 109, 110–16 (2023).

III. Legislative and Regulatory Developments

The FTC is not alone in its concern about the competition harms of surveillance pricing. Some state attorney generals are now investigating businesses' use of personal data to set individualized prices.[24] Further, state legislatures have moved to address these concerns, and federal proposals are now responding to that patchwork.

In California, lawmakers have advanced multiple approaches. Assembly Bill 446 would prohibit "surveillance pricing" in grocery establishments, defined as "offering or setting a customized price increase for a good or service for a specific consumer or group of consumers, based, in whole or in part, on personally identifiable information collected through electronic surveillance technology."[25] The bill provides that "only a public prosecutor . . . may bring an action" for penalties and that a consumer may "bring an action for injunctive relief."[26] The measure, however, remains on the Senate Inactive File.[27]

California's Senate Bill 259—the Fair Online Pricing Act—would separately prohibit setting prices based on a consumer's online device, including its "hardware state," "[t]he presence or absence of any software," or geolocation data, subject to exceptions (*e.g.*, device repairs, trade-in values, legitimate regional pricing, and real-time demand).[28] "[C]ellular broadcast technology" remains outside of the bill's scope because the Legislature found that it "is a critical service, especially during a state of emergency," and "does not use personal data."[29] Similar to Assembly Bill 446, the bill is pending on the Assembly Inactive File.[30]

Finally, while not a surveillance-pricing bill, Assembly Bill 325 was enacted in 2025 and amends the Cartwright Act to regulate algorithmic pricing.[31] The bill makes it "unlawful for a person to use or distribute a common pricing algorithm as part of a contract, combination . . . or conspiracy to restrain trade," and likewise unlawful where a person "coerces another person to set or adopt a recommended price" from such an algorithm.[32]

In New York, the legislature enacted the Algorithmic Pricing Disclosure Act, requiring disclosures when prices are set by an algorithm using personal data.[33] Litigation by the National Retail Federation challenged the mandated labels ("THIS PRICE WAS SET BY AN ALGORITHM USING

---

[24] *See, e.g.*, Press Release, *On Data Privacy Day, Attorney General Bonta Focuses on Surveillance Pricing, Compliance with California Consumer Privacy Act*, Office of Att'y Gen. Rob Bonta (Jan. 27, 2026), https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-focuses-surveillance-pricing-compliance; Press Release, *Attorney General James Demands Answers from Instacart about Algorithmic Pricing*, Office of N.Y. Att'y Gen. (Jan. 8, 2026), https://ag.ny.gov/press-release/2026/attorney-general-james-demands-answers-instacart-about-algorithmic-pricing.

[25] Cal. A.B. 446 (2025–26 Reg Sess.) (as amended Aug. 29, 2025) (pending Senate inactive file) (explaining that surveillance pricing includes "the use of technological methods, systems, or tools . . . that are capable of gathering personally identifiable information about a consumer's behavior, characteristics, location, or other personal attributes, whether in physical or digital environments").

[26] *Id.*

[27] *Id.*

[28] Cal. S.B. 259 (2025–26 Reg. Sess.).

[29] *Id.*

[30] *Id.*

[31] Cal. A.B. 325 (2025) (enacted); *see also* Brian Boyle et al., *Antitrust Meets AI: Plaintiffs, Enforcers, and Legislatures Take Aim at Alleged AI-Driven Collusion* (Nov. 14, 2025), https://www.dlapiper.com/en-us/insights/publications/2025/11/antitrust-and-ai-plaintiffs-enforcers-and-legislatures-take-aim-at-alleged-ai-driven-collusion.

[32] Cal. A.B. 325.

[33] Electronic Privacy Information Center (EPIC), *Amicus Briefs: National Retail Federation v. New York City*, https://epic.org/documents/national-retail-federation-v-james/ (last visited April 3, 2026).

YOUR PERSONAL DATA") as stigmatizing and a violation of the First Amendment.[34] The federal judge dismissed the case in October 2025 finding the law was "reasonably related to the government's legitimate interest in ensuring that customers are 'inform[ed]' about the terms on which products are offered to them, including the price."[35]

Other states have followed with targeted prohibitions and disclosures. Pennsylvania's Surveillance Pricing Act, House Bill 1942, would ban "[o]ffering or setting a customized price . . . based, in whole or in part, on personally identifiable information collected through electronic surveillance technology," and authorize a "civil penalty not to exceed $12,500 for each violation."[36] Minnesota's companion bills would prohibit using AI to "adjust, fix, or control product prices in real time based on market demands, competitor prices, inventory levels, customer behavior, or other factors."[37] Ohio's bill would bar distribution or use of a "pricing algorithm that uses, incorporates, or is trained with nonpublic competitor data."[38] Georgia's bill states: "No person shall engage in surveillance based price discrimination," with civil penalties up to $10,000 per violation and a private right of action.[39] Related proposals are pending in New York that would prohibit personalized algorithmic pricing in food and drug retail establishments and regulate algorithmically set prices, and other states (*e.g.*, Massachusetts, Vermont, Washington) have considered sectoral or disclosure-focused measures.[40]

Recent 2026 proposals specifically address dynamic and surveillance pricing. In New York, the proposed Protecting Consumers and Jobs from Discriminatory Pricing Act targets personalized algorithmic pricing in retail by banning electronic shelf labels, prohibiting personalized pricing and the use of "class data," and forbidding any personalization for minors.[41] It includes a broad private right of action (covering consumers, employees, and labor organizations), class actions, and remedies that include actual damages or statutory damages of at least $5,000 per violation, treble damages, and disgorgement.[42] In Minnesota, a pending bill would prohibit using AI to "adjust, fix,

---

[34] *Id.*

[35] Nat'l Retail Fed'n v. James, No. 25-cv-5500 (JSR), at 21 (S.D.N.Y. Oct. 8, 2025); Jonathan Stempel, *Judge Dismisses Retail Group's Challenge to New York Surveillance Pricing Law*, Reuters (Oct. 8, 2025), https://www.reuters.com/sustainability/boards-policy-regulation/judge-dismisses-retailing-groups-challenge-new-york-surveillance-pricing-law-2025-10-08/.

[36] Pa. H.B. 1942 (2025–26 Reg. Sess.). In the bill, the General Assembly cited a recent study documenting how businesses are "aggressively and secretly engaging in surveillance of their customers and . . . varying prices between customers and groups." *Id.* Findings included that "Mac users typically spend more money to stay at hotels . . . than non-Mac users"; "[h]otel booking sites charged people in certain zip codes more money to stay at hotels than people in other zip codes across the country"; and an office-supply store "charged people more for the same stapler if they knew a person had fewer options such as not being physically near a competitor." *Id.*

[37] Minn. H.F. 2452 (2025–26 Reg. Sess.); Minn. S.F. 3098 (2025–26 Reg. Sess.).

[38] Ohio S.B. 79 (2025–26 Reg. Sess.) (pending referral to committee).

[39] Ga. S.B. 164 (2025–26 Reg. Sess.).

[40] *See, e.g.*, N.Y. A. 9396 (banning personalized algorithmic pricing in food and drug retail); N.Y. S. 8616 (Senate companion banning personalized algorithmic pricing in food and drug retail); N.Y. A. 9349 (prohibiting algorithmically set prices and requiring automatedpricing disclosures); N.Y. S. 8623 (2025–26 Reg. Sess.) (Senate companion prohibiting algorithmically set prices and requiring disclosures); Mass. H. 99 (barring biometricbased surveillance pricing in grocery stores); Mass. S. 2515 (2025–26 Reg. Sess.) (Senate bill limiting biometric surveillance pricing in grocery stores); Vt. S. 207 (2025–26 Reg. Sess.) (prohibiting surveillance pricing using consumer data except in narrow circumstances); Wash. H.B. 2481 (2025–26 Reg. Sess.) (prohibiting surveillancebased price discrimination and surge pricing for retail goods).

[41] Ken Ryan et al., *2026 State AI Bills That Could Expand Liability, Insurance Risk*, Law360 (Jan. 13, 2026, 2:16 PM), https://www.law360.com/competition/articles/2428744/2026-state-ai-bills-that-could-expand-liability-insurance-risk- (citing Assemb. B. A9396, 2025-26 Reg. Sess. (N.Y. 2025)).

[42] *Id.*

or control" product prices in real time based on demand, competitor prices, inventories, customer behavior, or similar factors.[43] While nominally enforced by the Attorney General, Minnesota's Private Attorney General Act effectively enables private enforcement.[44] In North Carolina, a rent-setting bill would bar lessors and their agents from paying for or subscribing to "coordinating functions" that use nonpublic competitor data to recommend rental prices or terms via computational systems or algorithms, including AI, and would authorize damages (including punitive or treble damages) while invalidating forced arbitration agreements.[45]

Federal proposals have arisen in response to the state-by-state developments, progressing along two distinct pathways. First, members of Congress have floated bills to curb or prohibit consumer-facing surveillance pricing, including Rep. Greg Casar's Stop AI Price Gouging and Wage Fixing Act of 2025 and Sen. Kirsten Gillibrand's proposed One Fair Price Act.[46] Second, broader AI governance proposals—some of which aim to harmonize divergent state approaches—contemplate disclosure or constraints on automated decision-making that may capture pricing systems.[47]

Extending this federal–state dynamic beyond Congress, the White House's December 2025 Executive Order, Ensuring a National Policy Framework for Artificial Intelligence, directs the Department of Justice to form a task force to challenge state AI laws, Department of Commerce to catalogue conflicting state requirements, the Federal Communications Commission to consider a federal disclosure/reporting standard that would preempt state rules, and the FTC to issue a policy statement on when the FTC Act preempts state mandates that require "alterations to the truthful outputs of AI models."[48] The EO's framing could affect state algorithmic-pricing disclosure regimes and broader automated decision-making technology (ADMT) rulemakings, depending on how agencies implement it.

Internationally, the Organisation for Economic Co-operation and Development's (OECD) 2018 note on personalized pricing flagged risks of welfare loss and opacity, while pointing to data protection as a policy lever alongside competition tools.[49] The European Union's General Data Protection Regulation (GDPR) imposes transparency, lawful-basis, and profiling/automated-decision safeguards germane to individualized pricing, including Article 22 rights, subject to debated scope in affinity-based pricing.[50] Comparative analyses caution that strict data rules can have unintended competition consequences and distributional effects, sometimes strengthening incumbents with rich first-party data.[51]

---

[43] *Id.* (citing S. File 3098, 94th Leg., 2025-26 Sess. (Minn. 2025)).

[44] *Id.*

[45] *Id.* (citing H.B. 970, 2025-26 Sess. (N.C. 2025)).

[46] Gwendolyn J. Lindsay Cooley, *Getting Better at Algorithmic Pricing*, 40 Antitrust 34, 37–38 (2025) (discussing congressional proposals); Press Release, Office of Sen. Kirsten Gillibrand, *Gillibrand Introduced Bill to Crack Down on Surveillance Pricing* (Dec. 12, 2025), https://www.gillibrand.senate.gov/news/press/release/gillibrand-introduces-bill-to-crack-down-on-surveillance-pricing/ (announcing the One Fair Price Act, which would prohibit companies from using personal data to set individualized prices).

[47] *See* Laurie Harris, Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress, Lib. of Cong. (June 4, 2025), https://www.congress.gov/crs-product/R48555.

[48] DLA Piper, *New Executive Order Aims to Preempt State AI Regulation: Top Points* (Dec. 15, 2025), https://www.dlapiper.com/en-us/insights/publications/2025/12/new-executive-order-aims-to-preempt-state-ai-regulation.

[49] OECD Secretariat, *Personalised Pricing in the Digital Era*, DAF/COMP (2018), at 7–12, 26–30 (Nov. 20, 2018), https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf.

[50] W. Gregory Voss, *Surveillance Pricing and Personal Information*, 1 Antitrust Chron. 42, 43–48 (2025).

[51] *See* Ginger Zhe Jin et al., *Surveillance Pricing: A Cautionary Summary of Potential Harms and Solutions*, 1 Antitrust Chron. 17, 23 (2025).

IV. Current U.S. Legal Framework: Antitrust, Section 5, and Privacy

These emerging regulatory efforts unfold against the backdrop of longstanding U.S. legal doctrines that touch, at various points, on pricing and data use. To date, no federal statute comprehensively regulates the use of personal data to set consumer-specific prices in otherwise lawful settings. But existing tools reach adjacent conduct and constrain inputs.

First, Sherman Act Section 1. Algorithms alone do not immunize agreements: agreeing to outsource key pricing decisions to a common vendor, pool competitively sensitive non-public data, or align prices through a shared "hub" can support conspiracy theories under Section 1 of the Sherman Act. Recent litigation involving revenue management software in the multifamily and hospitality industries shows that courts and enforcers—through statements of interest—view delegating pricing to a software product as no shield from Section 1 liability.[52] In contrast, tools built on only public datapoints with unilateral use pose harder Section 1 questions absent plus factors, as courts have noted.[53] While to date these cases have focused on dynamic pricing models, their applicability would likely extend to common surveillance pricing models.

Second, Sherman Act Section 2. Dominant-firm misuse of unique data assets or widespread adoption of common intermediaries could support exclusionary theories. For example, targeted predation enabled by confining losses to switchers, or foreclosure via exclusive data arrangements—though surveillance-pricing-specific Section 2 cases remain nascent.[54] Economic commentary underscores structural sensitivities where rival-price inputs are central.[55]

Third, Robinson-Patman Act (RPA). The RPA prohibits price discrimination between different purchasers of commodities of "like grade and quality" in commerce and does not reach services or other non-commodity transactions, so it is a poor fit for online surveillance pricing.[56] Its secondary-line framework, and per se rules on discriminatory promotional payments and services, police wholesale favoritism, not individualized retail pricing.[57]

Following a Bedoya-led revival of RPA investigations during the Biden administration—including FTC actions against Southern Glazer's Wine & Spirits, LLC, and Pepsi—federal enforcement now appears dead on arrival under current leadership, with any remaining matters likely confined to traditional wholesale settings.[58] Some state attorneys general may pursue a red/blue divergence under state analogs or unfair-practices statutes, though the AI Executive Order may channel pricing-and-data issues into other regimes.[59] Private RPA suits face threshold hurdles (commodities-only scope, "like grade and quality," contemporaneous interstate sales, net-price parity, and competitive injury), making the RPA an unlikely vehicle to police surveillance pricing at scale.

---

[52] In re RealPage, Inc., Rental Software Antitrust Litig., 709 F. Supp. 3d 478, 493 (M.D. Tenn. 2023); Duffy v. Yardi Sys., Inc., 758 F. Supp. 3d 1283, 1292–93 (W.D. Wash. 2024); *see also* Statement of Interest of the United States, *RealPage, Inc.*, 709 F. Supp. 3d 478, https://www.justice.gov/d9/2023-11/418053.pdf; Statement of Interest of the United States, *Yardi*, 758 F. Supp. 3d 1283, https://www.ftc.gov/system/files/ftc_gov/pdf/YardiSOI-filed%28withattachments%29_0.pdf.

[53] Gibson v. Cendyn Grp., LLC, No. 2:23-cv-00140-MMD-DJA, 2024 U.S. Dist. LEXIS 83547, at *3–5 (D. Nev. May 8, 2024), *aff'd*, 148 F.4th 1069 (9th Cir. 2025).

[54] *See* Edward M. Iacobucci, *Algorithmic Pricing, Anticompetitive Counterfactuals, and Antitrust Law*, 91 U. Chi. L. Rev. (Online) (2024).

[55] *See, e.g.*, Brown & MacKay, *supra* note 23, at 110–16.

[56] 15 U.S.C. § 13(a).

[57] *Id.* § 13(d)–(e); FTC v. Morton Salt Co., 334 U.S. 37, 49–51 (1948).

[58] *See, e.g.*, FTC v. Southern Glazer's Wine & Spirits, LLC, No. 8:24-cv-02684, 2025 U.S. Dist. LEXIS 94533 (C.D. Cal. Apr. 17, 2025); FTC v. PepsiCo, Inc., No. 1:25-cv-00664, 2025 U.S. Dist. LEXIS 250856 (S.D.N.Y. Dec. 4, 2025).

[59] Exec. Order No. 14,110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75,191 (Nov. 3, 2023).

Fourth, FTC Act Section 5. The FTC can pursue unfair methods of competition and unfair or deceptive acts or practices that fall outside the Sherman Act's letter, including invitations to collude or dark patterns tied to opaque pricing practices, alongside its 6(b) authority to illuminate opaque markets.[60]

Fifth, privacy and data laws. Inputs matter. The federal Electronic Communications Privacy Act (ECPA) restricts interception or access to communications without consent, which could constrain surveillance-driven pricing flows that monitor communications.[61] State privacy laws (CCPA/CPRA and analogs) impose notice, purpose limits, and opt-out rights relevant to profiling; biometric statutes like BIPA add consent and handling constraints if such signals are used in pricing models.[62]

These combined tools can police collusion, deception, and unlawful data acquisition or use, yet leave a gap regarding otherwise lawful individualized price setting based on personal data absent other misconduct—hence the turn toward targeted transparency and input rules.

V. Investigations and Cases: Data Flows and Tooling

While direct "surveillance pricing" case law is lean, enforcement around data flows is instructive. The FTC's recent actions against location data brokers document how precise geolocation "reveals information about and details of consumers' lives that cannot be obtained through physical observations of public spaces," and how brokers' products "identify sensitive characteristics about consumers."[63] For example, the *Gravy Analytics* complaint quotes Venntel marketing that location data reveals "patterns-of-life (POL), locations visited and known associates," including identifying a user's "bed down location" and "work location."[64] Further, the complaint alleges respondents "sold, licensed, or otherwise transferred precise geolocation data associated with unique persistent identifiers that reveal consumers' visits to sensitive locations," concluding that the unauthorized collection and sale of such data is an "unwarranted intrusion into consumers' privacy."[65]

The *Mobilewalla* matter involves similar data pipelines, with additional emphasis on real-time bidding. The FTC alleges *Mobilewalla* built geo-fenced audience segments tied to highly sensitive locations and events, retained detailed location information, and failed to take reasonable steps to verify suppliers' consent representations.[66] In their joint statement, the Chair and two Commissioners describe RTB-based bidstream harvesting as "shockingly commonplace" and an "outrageous

---

[60] Fed. Trade Comm'n, Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 (Nov. 10, 2022); Fed. Trade Comm'n, Bringing Dark Patterns to Light (Sept. 2022).

[61] *See* U.S. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22, 2701-12.

[62] *See, e.g.*, Cal. Civ. Code §§ 1798.100-.199.95; 740 Ill. Comp. Stat. 14/1-14/99.

[63] Press Release, Fed. Trade Comm'n, *FTC Finalizes Order Prohibiting Gravy Analytics, Venntel from Selling Sensitive Location Data* (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-prohibiting-gravy-analytics-venntel-selling-sensitive-location-data; Complaint, In re Gravy Analytics, Inc. & Venntel, Inc., FTC Matter No. 212-3035 ¶¶ 25, 57, 69 (Apr. 2024).

[64] Complaint, *In re Gravy Analytics, Inc.*, FTC Matter No. 212-3035 ¶¶ 25, 57, 69 (Apr. 2024).

[65] *Id.* ¶¶ 59, 73.

[66] Complaint, In re Mobilewalla, Inc., FTC Matter No. 2023196 ¶¶ 12–15, 27–32, 70, 74 (Dec. 3, 2024).

privacy violation," emphasizing that firms can capture and retain web browsing and location data "even when [they do] not serve any ads."[67]

Orders in analogous matters have imposed structural remedies. In *X-Mode/Outlogic*, the Commission secured a "first-time ban on the use, sale, or disclosure of sensitive location data," together with deletion of unlawfully collected data and derived models and a Sensitive Location Data Program and Supplier Assessment Program.[68] *InMarket*'s complaint likewise details long-term retention and undisclosed profiling via SDKs and third-party app integrations, noting that location permissions in utility apps can trigger downstream collections by third parties that aggregate sensitive data.[69]

VI. Economics and Welfare: Mixed Effects and Distributional Concerns

But surveillance pricing is not uniformly condemned. The academic literature does not render a single verdict. Under competitive conditions, individualized pricing can expand output and intensify competition for elastic consumers.[70] Surveyed evidence in recent commentary suggests that a substantial share of consumers may pay less than under uniform pricing, though gains are distributional and context-dependent.[71] Personalization can reduce deadweight loss by bringing marginal consumers into the market and by aligning discounts with willingness to pay, especially when firms face heterogeneous demand and meaningful marginal costs.[72]

At the same time, increased granularity can enable surplus extraction from inelastic buyers, while opacity may erode trust and choice.[73] Reliance on high-frequency inputs about rivals' prices can also soften competition at market scale, raising average prices even as dispersion increases.[74] Risks are heightened when common tools process shared or correlated signals about competitors' prices or when rapid, automated matching dampens incentives to undercut.

Distributional and equity concerns further complicate welfare analysis. Even without using protected traits directly, behavioral, location, and device proxies can correlate with protected characteristics and produce disparate impacts.[75] These effects can be most acute when data access is asymmetric or when personalization is layered on market power, potentially making outcomes regressive for consumers with fewer outside options or more inelastic demand.[76] "Perceptions of unfairness" can also reduce consumer surplus by deterring participation or inducing costly search and avoidance.[77]

---

[67] Statement of Chair Lina M. Khan, Joined by Comm'rs Bedoya & Slaughter, In re Mobilewalla, Inc. 1–2 (Dec. 3, 2024); *see also* Dissenting Statement of Comm'r Melissa Holyoak, In re Mobilewalla, Inc. (Dec. 3, 2024); Concurring and Dissenting Statement of Comm'r Andrew N. Ferguson, In re Gravy Analytics, Inc. & In re Mobilewalla, Inc. 1–4 (Dec. 3, 2024).

[68] Statement of Chair Lina M. Khan & Comm'rs Slaughter & Bedoya, In re X-Mode Social, Inc. & Outlogic, LLC, at 2 (Jan. 9, 2024); Decision and Order, X-Mode Social, Inc. & Outlogic, LLC, Part II–III (Jan. 9, 2024).

[69] Complaint, In re InMarket Media, LLC ¶¶ 6–11, 15–17, 23.

[70] Rebecca Kirk Fair et al., *The Rise of Surveillance Pricing*, 1 Antitrust Chron. 25, 25–31 (2025).

[71] *Id.*

[72] *Id.* at 36; Yun, *supra* note 4, at 9.

[73] *See* Jin et al., *supra* note 51, 19–20; Fair et al., *supra* note 70, at 29.

[74] Zach Y. Brown & Alexander MacKay, *Data and Price Competition: The Special Role of Information About Rivals' Prices*, 1 Antitrust Chron. 12, 14–16 (2025).

[75] Fair et al., *supra* note 70, at 29–30.

[76] *Id.*

[77] Jin et al., *supra* note 73, at 19.

These trade-offs counsel calibrated design by both regulators and companies designing pricing programs. Blunt prohibitions risk foreclosing beneficial personalization and entrenching incumbents.[78] Regulators may find that targeted prohibitions of specific inputs and transparency requirements may preserve efficiency gains while mitigating opacity and coordination risks.[79] For corporate compliance, targeted guardrails on inputs such as rivals' prices and common tooling, transparency about salient signals, and documentation of testing and monitoring will be critical.[80] Amidst the currently applicable patchwork framework of rules, it will be critical for companies and associated third-party intermediaries to ensure compliance.[81]

VII. Practice Guidance: A Calibrated Governance Playbook

Taken together, these cases and policy trends highlight the need for practical governance strategies. Given the ever-changing legislative landscape in this area, companies evaluating or operating pricing systems that rely on consumer data are encouraged to seek legal guidance. That said, for companies evaluating or operating pricing systems that rely on consumer data, it is advisable for companies to adopt some practical measures to ensure compliance with the most notable trends in enforcement—a governance playbook.

- **Control inputs and access.** For surveillance pricing systems, exclude sensitive personal information (*e.g.*, precise geolocation, device state, biometrics) from price-setting inputs; strictly firewall any competitor data; avoid high-frequency ingestion of rivals' prices that can raise competition-softening concerns; and require vendor contracts to prohibit cross-client data pooling or leakage tied to individualized prices.
- **Maintain meaningful human oversight.** Retain authority to override individualized price recommendations; implement guardrails tailored to surveillance signals (price ceilings/floors, day-over-day caps, anomaly alerts); require exception review and contemporaneous business justifications where surveillance-derived inputs materially increase a consumer's price.
- **Test and monitor.** Run periodic audits for disparate impact across protected or proxy groups; monitor for anomalous price dispersion patterns linked to surveillance signals; document remediation; and align the cadence of testing to use-case risk, market power, and repricing frequency.
- **Transparency and consumer communication.** Where state law requires, disclose when personal or device data materially influence a price; avoid relegating material practices to privacy policies alone; provide clear, at-point-of-interaction explanations sufficient for a reasonable consumer to understand how surveillance signals affect price and available choices.
- **Vendor diligence.** If using third-party tools, confirm whether they generate individualized prices; obtain documentation of input signals, data sources, and objective functions; require the ability to disable surveillance-oriented signals (*e.g.*, device hardware state, geolocation-based inferences); and prohibit cross-context behavioral use for pricing without explicit authorization.
- **Align with privacy-by-design.** Map pricing data flows end-to-end; minimize personal data to what is necessary for pricing; ensure lawful basis, notice, and rights management consistent

---

[78] *Id.* at 19–22.

[79] Fair et al., *supra* note 70, at 9; Brown & MacKay, *supra* note 74, at 15–16.

[80] *See* Brown & MacKay, *supra* note 74, at 15–16.

[81] *See* Tonya Riley, *State Data-Driven Pricing Bans Spark Industry Pushback*, Bloomberg L. (Apr. 21, 2026, 5:00 AM), https://news.bloombergtax.com/us-law-week/state-data-driven-pricing-bans-spark-industry-pushback.

with applicable state privacy statutes; and apply heightened controls to location and biometric signals given elevated legal and enforcement risk.[82]

Conclusion

Surveillance pricing is not merely a new label for dynamic pricing; it is a data-intensive frontier that marries individual-level signals to automated pricing choices, often via intermediaries. The FTC's 6(b) inquiry has surfaced early, concrete examples of the data and tools in play while candidly acknowledging limits and open questions. Absent a comprehensive federal statute, U.S. governance will continue to rely on a mix of antitrust, Section 5, and privacy constraints—augmented by targeted state efforts—to police collusion, deception, unlawful data use, and the most sensitive forms of surveillance pricing.

Is it all bad? Not necessarily. Economic literature has long recognized that price discrimination can increase total output and, under certain conditions, benefit consumers, although with certain trade-offs. These mixed effects argue for calibrated guardrails rather than categorical bans. Targeted transparency can preserve many of the efficiency gains associated with algorithmic pricing while mitigating the most salient risks. Ultimately, the policy challenge is to channel powerful new pricing capabilities toward procompetitive and pro-consumer uses, and to do so in a way that is legible to the people who pay the prices. ●

[82] For an additional tool with which to assess AI systems, see AI Markets (AIM) Toolkit, Competition & Consumer Comm'n Singapore, https://www.ccs.gov.sg/resources/ai-markets-toolkit/ai-markets--aim--toolkit/.