THE RISE OF SURVEILLANCE PRICING

BY REBECCA KIRK FAIR, ALVARO ZIADI & JUAN CARVAJAL[1]



1 Rebecca Kirk Fair is a Managing Principal at Analysis Group, Inc.; Alvaro Ziadi is a Manager at Analysis Group, Inc; Juan Carvajal is a Manager at Analysis Group, Inc. We thank Alicia Gong and Hufsa Ahmed from Analysis Group for their assistance. The views expressed here are those of the authors and do not necessarily reflect the views of Analysis Group, its affiliates, or its clients.

CPI ANTITRUST CHRONICLE
July 2025

SHOULD WE FEAR PERSONALIZED PRICING?
By John M. Yun

DATA AND PRICE COMPETITION: THE SPECIAL ROLE OF INFORMATION ABOUT RIVALS' PRICES
By Zach Y. Brown & Alexander MacKay

SURVEILLANCE PRICING: A CAUTIONARY SUMMARY OF POTENTIAL HARMS AND SOLUTIONS
By Ginger Zhe Jin, Liad Wagman & Mengyi Zhong

THE RISE OF SURVEILLANCE PRICING
By Rebecca Kirk Fair, Alvaro Ziadi & Juan Carvajal

PERSONALIZED PRICING: ANTITRUST AND POLICY CONSIDERATIONS IN THE AGE OF PERSONALIZATION
By Gabriela Antonie, J.P. Bruno, Mariella Gonzalez & Esperanza Johnson

SURVEILLANCE PRICING AND PERSONAL INFORMATION
By W. Gregory Voss

INFLATION'S SPIES: THE LABOR OF SURVEILLANCE PRICING
By Aaron Shapiro

Visit www.competitionpolicyinternational.com for access to these articles and more!

THE RISE OF SURVEILLANCE PRICING

By Rebecca Kirk Fair, Alvaro Ziadi & Juan Carvajal

The Federal Trade Commission ("FTC") and international regulators have launched inquiries into the use of "surveillance pricing," practices in which firms use detailed consumer data and algorithmic tools to set individualized prices and steer product offerings. We examine these evolving practices and the tension between, on the one hand, the efficiencies and improved market access that such practices can enable and, on the other, the legal and policy questions raised by their proliferation. Specifically, the FTC is concerned that such practices may lead to discriminatory outcomes, privacy violations, or algorithmic collusion. From a legal perspective, the article highlights the competing demands of innovation and consumer protection, particularly in contexts in which there is a lack of transparency or meaningful consent. We also review the economic rationale for personalized pricing, consider the distributional and competitive effects of these models, and explore the regulatory frameworks – such as the FTC's Section 6(b) authority and the EU's GDPR – that are being tested by surveillance pricing. We conclude by underscoring the need for empirical research and regulatory clarity as data-driven pricing technologies continue to advance.

With the increased digitization of the economy and consumers' everyday lives, many companies across a wide array of sectors increasingly rely on algorithms, coupled with extensive consumer data collection, for personalized price setting. Take, for example, a person who wants to buy plane tickets to visit family. Most likely, this person will go online, search for ticket prices, perhaps monitor them over time, and purchase a ticket at a given price. A different person, with a different browsing and location history, looking for the same ticket will most likely be faced with a different price. This phenomenon is referred to as "surveillance pricing," a practice that relies on "large-scale data collection to help sellers maximize their revenues by customizing the pricing, as well as the selection of products and services, offered to each consumer."[2]

Surveillance pricing practices commonly result in different consumers being offered different prices for the same product, depending on data collected about the consumers. The type of data used by companies to set individualized prices varies, but it can include location;[3] the device used by the consumer,[4] as well as its operating system, browser,[5] and language;[6] and the consumer's history of browsed and purchased products.[7] For example, Target has been reported to offer customers different prices on the Target app depending on whether the customer was located inside or outside a store.[8]

Other times, surveillance pricing practices result in different consumers being offered different products altogether, based on the data collected about them, a practice referred to as "steering."[9] For example, after an online travel agency found that Apple's Mac users were willing to pay up to 30 percent more on hotels than Windows users, they started showing Apple's Mac users costlier travel options than Windows users.[10] This practice is not uncommon, and many e-commerce platforms' product recommendations depend on the data collected on specific users.[11]

And the use of surveillance pricing is rising. For example, Amazon, where 35 percent of all retail sales are expected to occur by 2027,[12] uses real-time data to tailor its offerings depending on customers' preferences, browsing histories, and purchase behaviors.[13] However, surveillance pricing is also common in many other industries, such as transportation network companies,[14] online test preparation services,[15] office supply retailers,[16] broadband internet services,[17] and travel vendors.[18]

---

2 *Issue Spotlight: The Rise of Surveillance Pricing*, FEDERAL TRADE COMMISSION (2025), https://www.ftc.gov/system/files?file=ftc_gov/pdf/sp6b-issue-spotlight.pdf ("Issue Spotlight"), at 2.

3 Jakub Mikians, et al., *Detecting Price and Search Discrimination on the Internet*, PROCEEDINGS OF THE 11TH ACM WORKSHOP ON HOT TOPICS IN NETWORKS, 79–84 (2012).

4 Aniko Hannak, et al., *Measuring Price Discrimination and Steering on E-commerce Web Sites*, PROCEEDINGS OF THE 2014 CONFERENCE ON INTERNET MEASUREMENT CONFERENCE, 305–318 (2014).

5 Thomas Hupperich, et al., *An Empirical Study on Online Price Differentiation*, PROCEEDINGS OF THE EIGHTH ACM CONFERENCE ON DATA AND APPLICATION SECURITY AND PRIVACY, 76–83 (2018).

6 Hupperich, *supra* note 5.

7 Hannak, *supra* note 4.

8 Casey Bond, *Target is Tracking You and Changing Prices Based on Your Location*, HUFFPOST (2022), https://www.huffpost.com/entry/target-tracking-location-changing-prices_l_603fd12bc5b6ff75ac410a38.

9 Issue Spotlight, at 11.

10 Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, THE WALL STREET JOURNAL(2012), https://www.wsj.com/articles/SB10001424052702304458604577488822667325882.

11 Nan Chen & Hsin-Tien Tsai, *Steering Via Algorithmic Recommendations*, THE RAND JOURNAL OF ECONOMICS, 55(4), 501–518 (2024).

12 Kate Gibson, *Dynamic Pricing: What It Is & Why It's Important*, HARVARD BUSINESS SCHOOL ONLINE (2024), https://online.hbs.edu/blog/post/what-is-dynamic-pricing.

13 Nadica Naceva, *The Ultimate Guide to Amazon Dynamic Pricing Strategy in 2024*, INFLUENCER MARKETING HUB (2024), https://influencermarketinghub.com/amazon-dynamic-pricing/.

14 Gaby Del Valle, *Are You Being Exploited by AI-Powered Surveillance Pricing?*, THE VERGE (2024), https://www.theverge.com/2024/7/23/24204011/ftc-surveillance-pricing-investigation-mckinsey-mastercard-chase. Henry Chandonnet, *The FTC Is Cracking Down on Surveillance Pricing. Experts Are Still Divided on Whether It's Really So Bad*, FAST COMPANY (2024), https://www.fastcompany.com/91161417/ftc-cracking-down-on-surveillance-pricing-experts-weigh-in.

15 Keyon Vafa, et al., *Price Discrimination in the Princeton Review's Online SAT Tutoring Service*, TECHNOLOGY SCIENCE (2015), https://techscience.org/a/2015090102/.

16 Jennifer Valentino-DeVries, et al., *Websites Vary Prices, Deals Based on Users' Information*, THE WALL STREET JOURNAL (2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

17 Leon Yin & Aaron Sankin, *Dollars to Megabits, You May Be Paying 400 Times as Much as Your Neighbor for Internet Service*, THE MARKUP (2022), https://themarkup.org/still-loading/2022/10/19/dollars-to-megabits-you-may-be-paying-400-times-as-much-as-your-neighbor-for-internet-service.

18 Mikians, *supra* note 3.

The rise of surveillance pricing has brought greater public scrutiny, as well as increased attention from both regulators and economists, to this practice. In this article, we first outline recent regulatory concerns surrounding surveillance pricing and then review economic findings on its benefits and potential risks.

I. REGULATORY AND ENFORCEMENT FOCUS

Academic research has highlighted that personalized pricing can increase firm revenue and expand access for price-sensitive consumers, even as its effects on overall consumer surplus remain mixed.[19] Nevertheless, in recent years, the Federal Trade Commission ("FTC") has intensified its scrutiny of pricing practices that heavily rely on the use of user data and automated algorithms. While the FTC acknowledges the existence of "business value" gains from these tools, including their potential to maximize revenue and lower the costs of setting and changing prices,[20] it has also raised concerns that these tools may also lead to anticompetitive outcomes by facilitating price coordination among competitors or discriminatory pricing.[21] Former FTC Chair Lina Khan, for example, expressed concerns that firms could be exploiting Americans' personal data and "the possibility of each of us being charged a different price based on what firms know about us."[22]

As a result of these concerns, and under its 6(b) authority, the FTC initiated an investigation of surveillance pricing in July 2024, focusing on how companies, including retailers and third-party intermediaries, leverage detailed personal consumer data to tailor individualized prices for goods and services.[23] The goal of this investigation is three-fold:

- To understand what types of consumer data are being collected and how this data is leveraged for pricing decisions[24]
- To assess whether surveillance pricing strategies can lead to discriminatory practices, such as charging different prices for the same product based on consumers' personal characteristics[25]
- To evaluate how surveillance pricing systems operate and how they can affect consumers and market outcomes[26]

As part of this investigation, the FTC issued orders to eight firms — Mastercard, Revionics, Bloomreach, JPMorgan Chase, Task Software, PROS, Accenture, and McKinsey & Co. — that advertise the use of algorithms and AI to target prices to individual consumers.[27] These orders sought detailed information on: a) the types of surveillance pricing products developed by each of these companies; b) the data sources and data collection methods employed; c) information on the customers purchasing these surveillance pricing products; and d) the potential effect on the prices paid by consumers.[28]

In January 2025, the FTC released preliminary findings of its ongoing study. These initial findings suggest that a wide array of consumer data, ranging from consumers' "precise location or browser history" to "mouse movements on a webpage," are being collected and leveraged to set targeted and tailored prices.[29] Concurrently, the FTC released an "Issue Spotlight" in which the four main concerns related to surveillance pricing were outlined:[30]

19 Jean-Pierre Dubé & Sanjog Misra, *Personalized Pricing and Consumer Welfare*, *JOURNAL OF POLITICAL ECONOMY*, 131(1), 131–189 (2023).

20 *FTC Surveillance Pricing 6(b) Study: Research Summaries: A Staff Perspective*, FEDERAL TRADE COMMISSION (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf ("Staff Perspective").

21 Diane Hazel, et al., *FTC Issues Warning on the Use of Algorithms to Recommend or Set Prices*, FOLEY & LARDNER LLP (2024), https://www.foley.com/insights/publications/2024/03/ftc-warning-algorithms-recommend-set-prices/. Christopher Finnerty & Sheina Lefkowitz, *What Really Is Surveillance Pricing? The FTC Is Trying to Figure Out*, K&L GATES (2024), https://www.klgates.com/What-Really-is-Surveillance-Pricing-The-FTC-is-Trying-to-Figure-it-Out-8-2-2024.

22 Anna-Louise Jackson, *Lina Khan Says the FTC is Investigating Surveillance Pricing. Here's How That Could Affect You*, FAST COMPANY (2024), https://www.fastcompany.com/91195551/lina-khan-ftc-federal-trade-commission-chair-surveillance-pricing-explained-what-is-it.

23 *FTC Issues Orders to Eight Companies Seeking Information on Surveillance Pricing*, FEDERAL TRADE COMMISSION (2024), https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-issues-orders-eight-companies-seeking-information-surveillance-pricing ("FTC Issues Orders").

24 Staff Perspective, at 3; FTC Issues Orders.

25 FTC Issues Orders.

26 Staff Perspective, at 3; FTC Issues Orders.

27 FTC Issues Orders.

28 FTC Issues Orders.

29 *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices*, FEDERAL TRADE COMMISSION (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.

30 Issue Spotlight, at 12-15.

1. Privacy intrusion and opaque data collection: Intermediaries can compile a vast array of consumer information, from geographical location to sensitive personal characteristics, often without clear notice or meaningful opt-out mechanisms. This lack of notice or consumer control can create the potential to exploit vulnerable populations.
2. Discrimination against disadvantaged groups: Algorithms trained on historical data or demographic data can inadvertently, and sometimes systematically, discriminate against disadvantaged groups.
3. Extraction of consumer surplus: By estimating each potential buyer's maximum willingness to pay, firms can charge higher prices on those who are deemed less price-sensitive, causing some consumers to unknowingly pay more.
4. Anticompetitive risks through algorithmic collusion: When multiple sellers rely on common data or third-party algorithms, individualized pricing may constitute de facto collusion. Shared models or synchronized data inputs may align price adjustments across firms – replicating the anticompetitive harms of explicit price-fixing agreements even without direct human coordination.

However, as of January 2025, the FTC has withdrawn its request for public comments, effectively pausing further public inquiry into surveillance pricing.[31]

The FTC is not the only agency investigating surveillance pricing practices. Global regulators such as the UK's Competition and Markets Authority ("CMA") have raised similar concerns. The CMA, in a 2018 report, flagged algorithmic personalized pricing as a competition and consumer risk, noting that, while there was limited evidence of real personalized pricing in practice, algorithms were already used to personalize rankings, advertisements shown, and discounts offered.[32] Similar to the FTC, the CMA has acknowledged that surveillance and personalized pricing can be beneficial in many cases for both consumers and suppliers, due to their ability to reduce transaction costs and frictions, allow new entrants to compete, improve inventory management, and reduce consumers' search and transaction costs.[33] However, the increasing availability of data and sophisticated pricing algorithms pose many risks for competition, including price discrimination, lack of transparency, and loss of consumers' trust.[34]

II. SURVEILLANCE PRICING THROUGH AN ECONOMIC LENS: BENEFITS AND RISKS

From an economics perspective, surveillance pricing strategies are not new, and build on longstanding economic principles of price discrimination, which are widely understood to have the potential for increasing both consumer and total welfare. Notwithstanding the potential benefits arising from output expansion and increased access that can be brought about through price discrimination generally, the scale, speed, and potential opacity of today's data-driven pricing models introduce new tradeoffs, which economists have studied. While some economists point to enhanced efficiency and market access, others caution that such models could reinforce inequality, distort competition, and undermine consumer autonomy under some scenarios. In this section, we review the theoretical arguments from both perspectives and discuss some of the nuances embedded in each.

A. The Case for Price Discrimination: Efficiency and Personalization

At a foundational level, surveillance pricing is an extension of third-degree price discrimination — charging different prices to different consumers based on observable attributes.[35] Unlike traditional approaches that segment customers using broad categories like age or occupation, surveillance pricing uses individualized behavioral and contextual data — such as device type, browsing behavior, and location — to estimate willingness to pay ("WTP") and tailor prices accordingly.[36]

Economists have shown that price discrimination, when implemented effectively, can improve both firm efficiency and consumer access. Marshall (2015), for example, shows that targeting price-sensitive consumers with lower prices — when those consumers self-select into

31 *Statement Regarding Request for Public Comment Re: Surveillance Pricing Practices*, FEDERAL TRADE COMMISSION (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/khan-statement-regarding-request-for-public-comment-re-surveillance-pricing-practices.pdf.

32 *Pricing Algorithms: Economic Working Paper on the Use of Algorithms to Facilitate Collusion and Personalised Pricing*, UK COMPETITION & MARKETS AUTHORITY (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf ("CMA Economics Working Paper").

33 CMA Economics Working Paper, at 20-21, 35.

34 CMA Economics Working Paper, at 49-50.

35 Hal R. Varian, *Microeconomic Analysis*, 3rd ed. (New York: W.W. Norton & Company, 1992), 242 ("Third-degree price discrimination means that different purchasers are charged different prices, but each purchaser pays a constant amount for each unit of the good bought. This is perhaps the most common form of price discrimination; examples are student discounts, or charging different prices on different days of the week.").

36 Staff Perspective.

discount programs through higher hassle costs — can lead to welfare gains.[37] Betancourt et al. (2022) provide further support in the airline industry context, where dynamic pricing helps fill unsold seats, increases total output, improves capacity utilization, and raises consumer surplus.[38]

This logic applies broadly to industries with high fixed costs and perishable inventory, such as entertainment, travel, and ridesharing. Leslie (2004), for example, analyzed Broadway theater ticketing and found that price discrimination increased producer revenues by approximately 5 percent and tends to promote higher overall attendance compared to uniform pricing, though it did not lead to a measurable change in consumer welfare.[39]

Cohen (2008) offers a related example from the consumer goods market. The author's study of the paper towel industry shows that firms used package size to segment consumers with different price sensitivities, with an estimated 34–46 percent of unit price variation consistent with second-degree price discrimination.[40] While this strategy did not involve real-time or behavioral targeting, it illustrates the broader principle: Firms can extract more value from consumers by offering valuable product variants that appeal to different elasticity segments.

Surveillance pricing builds on these foundations. Rather than relying on physical packaging or purchase timing, firms now use real-time signals to refine price discrimination and optimize revenues. However, whether these strategies introduce meaningful consumer welfare improvements or competitive benefits remains an open question and requires further empirical study.

B. What's Different Now: Data Scale, Transparency, and Targeting

Notwithstanding the potential benefits arising generally from price discrimination, surveillance pricing differs from traditional forms of price discrimination in important ways. Most notably, it relies on real-time, large-scale data extraction and machine learning models that are sometimes opaque to both consumers and regulators. Whereas earlier forms of price discrimination were relatively transparent and static (e.g., student discounts), today's pricing models operate in "black box" environments where consumers typically do not know that prices are being tailored to them or what variables and information collected about them are driving those decisions.

This potential opacity complicates consumer choice and market discipline. If shoppers do not understand why they are being offered a particular price — or whether other consumers are being offered different prices — they may find it harder to trust firms or make informed decisions. As noted above, the FTC's 6(b) study on surveillance pricing raises concerns about the lack of transparency and the role of large-scale behavioral data collection in shaping both prices and product offerings.[41]

This concern extends beyond pricing to the "steering" practices discussed above. Notably, researchers have documented cases of online platforms altering the order or visibility of products based on factors like device type, browsing history, or user membership and login status.[42] This expands the reach of surveillance pricing beyond what consumers pay to what choices they see — potentially raising concerns about both fairness and autonomy.

C. Risks to Equity: Socioeconomic and Demographic Disparities

Economists and regulators have increasingly raised concerns that surveillance pricing could disproportionately impact marginalized groups. These concerns arise even when protected traits like race or gender are not used directly. As both Porat (2025) and the FTC's 6(b) study note, firms often rely on behavioral proxies — such as location history, purchase patterns, and browsing data — that can correlate with social identity and lead to disparate impacts.[43]

---

37 Guillermo Marshall, *Hassle Costs and Price Discrimination: An Empirical Welfare Analysis*, AMERICAN ECONOMIC JOURNAL: APPLIED ECONOMICS, 7(3), 123–146 (2015).

38 Jose M. Betancourt, et al., *Dynamic Price Competition: Theory and Evidence from Airline Markets (NBER Working Paper No. 30347)*, NATIONAL BUREAU OF ECONOMIC RESEARCH (2022).

39 Phillip Leslie, *Price Discrimination in Broadway Theater*, THE RAND JOURNAL OF ECONOMICS, 35(3), 520–541 (2004).

40 Andrew Cohen, *Package Size and Price Discrimination in the Paper Towel Market*, INTERNATIONAL JOURNAL OF INDUSTRIAL ORGANIZATION, 26(2), 502–516 (2008). See also Jose M. Betancourt, et al., *Dynamic Price Competition: Theory and Evidence from Airline Markets (NBER Working Paper No. 30347)*, NATIONAL BUREAU OF ECONOMIC RESEARCH (2022).

41 Staff Perspective, at 8-9; Issue Spotlight, at 12-13.

42 Hannak, *supra* note 4.

43 Haggai Porat, *Behavior-Based Price Discrimination and Data Protection in the Age of Algorithms*, THE JOURNAL OF LEGAL STUDIES (forthcoming 2025), at 33-34. See also, Staff Perspective.

Experimental research by Jacob et al. (2022) adds nuance to this concern. The study finds that low-socioeconomic-status consumers are less price-sensitive when they perceive a risk of discrimination. In upscale retail settings, these consumers were more likely to accept high prices and lower-value rewards, suggesting that surveillance pricing might exploit internalized expectations of exclusion. However, the authors also found that corporate social inclusion cues could help restore price sensitivity among these consumers — highlighting the role of firm messaging in shaping outcomes and ameliorating the aforementioned potential challenges.[44]

Additional empirical research also suggests that personalized pricing can have redistributive qualities that could be desirable if equality is more heavily weighted than efficiency. Dubé and Misra (2023) find that while such pricing strategies can reduce total consumer surplus, a significant portion of consumers – more than 60 percent, in their study – actually benefit from lower prices under personalization.[45] This complexity underscores the importance of considering distributional impacts when evaluating the fairness and welfare implications of surveillance pricing models.

While the effects discussed above may not be universal or uniform, they raise meaningful questions about fairness. Can consumers meaningfully consent to surveillance pricing models that adapt in real time based on inferred traits? And what happens from an inequality standpoint when these models "learn" to charge more to those least equipped to contest price?

D. Market Dynamics and Potential Competition Risks

The adoption of surveillance pricing also reshapes competitive dynamics. Larger firms with superior data access and modeling capabilities may enjoy significant advantages over smaller rivals. This could raise barriers to entry and entrench incumbents, especially in digital markets where scale effects and network externalities are already pronounced.

There is also concern about the potential for algorithmic collusion. While traditional price-fixing requires coordination, surveillance pricing tools — particularly when deployed across platforms — could produce "tacit collusion" as algorithms learn to avoid price wars and optimize profits.[46] Scholars like Ezrachi and Stucke have also warned of this risk.[47]

The Department of Justice recently sued RealPage over allegations that its rent pricing software facilitated an anti-competitive algorithmic pricing scheme.[48] Notably, however, those allegations focus on the centralized use of proprietary data across firms rather than consumer-facing price personalization. As such, the RealPage matter differs in important respects from the individualized pricing practices examined in the FTC's 6(b) study.

E. Privacy and Consent: The Regulatory Challenge

Surveillance pricing also raises questions around data privacy and informed consent. Consumers may not always be aware of what data are being collected, how they are used, or how its use influences the prices they are offered. Even if consumers are aware, it can be challenging for them to understand how their data influence the prices they see, since surveillance pricing practices are often complex and opaque.[49]

---

44 Jorge Jacob, et al., *Expected Socioeconomic-Status-Based Discrimination Reduces Price Sensitivity Among the Poor*, JOURNAL OF MARKETING RESEARCH, 59(6), 1083–1100 (2022).

45 Jean-Pierre Dubé & Sanjog Misra, *Personalized Pricing and Consumer Welfare*, JOURNAL OF POLITICAL ECONOMY, 131(1), 131–189 (2023).

46 CMA Economic Working Paper, at 45; *Algorithms and Collusion*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (2017), https://one.oecd.org/document/DAF/COMP/WD(2017)41/En/pdf. *Personalised Pricing in the Digital Era*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (2018), https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf.

47 CMA Economic Working Paper, at 45.

48 *Justice Department Sues RealPage for Algorithmic Pricing Scheme that Harms Millions of American Renters*, US DEPARTMENT OF JUSTICE (2024), https://www.justice.gov/opa/pr/justice-department-sues-realpage-algorithmic-pricing-scheme-harms-millions-american-renters.

49 This general observation is supported by both academic and regulatory literature. See Issue Spotlight.

In the EU, the General Data Protection Regulation ("GDPR") offers a relatively comprehensive legal framework that addresses profiling and requires transparency in automated decision making.[50] Nevertheless, as Li (2022) discusses, current EU protections face limitations when applied to affinity-based pricing models that rely on inferred characteristics or opaque data processing.[51]

In the US, the regulatory landscape is more fragmented. Li (2024) observes that the US approach is sector-specific and lacks uniform safeguards across industries, which can result in uneven coverage and potential gaps in consumer protection.[52]

Importantly, transparency about the use of algorithmic pricing has the potential to empower consumers by making digital markets more navigable and responsive. Porat's (2025) experimental research examines how individuals respond when they are explicitly informed about algorithmic price discrimination. The study finds that transparency significantly increases the likelihood that consumers will attempt to negotiate lower prices — suggesting that, in some contexts, disclosure and transparency can enhance consumer agency and improve bargaining outcomes.[53]

III. CONCLUSION & NEXT STEPS

Surveillance pricing sits at the intersection of innovation, privacy, competition, and fairness. With firms increasingly relying on detailed consumer data and automated algorithms to personalize pricing, economists and regulators have started to study the impact of these pricing practices. This question is not straightforward. Personalized pricing can increase efficiency, allowing firms to dynamically respond to changing market conditions and potentially broaden market access to previously unserved populations. Yet these same tools also raise pressing concerns about transparency, discriminatory pricing, privacy, and the potential for algorithmic collusion.

Regulators, including the FTC and CMA, have begun scrutinizing how these pricing models function in practice and the extent to which they may benefit or harm consumers. While their investigations acknowledge the efficiency-enhancing potential of algorithmic price discrimination, they also highlight substantial risks — particularly in contexts where data use is opaque or inferences lead to disparate treatment among consumers.

For economists and policymakers, the path forward involves navigating a nuanced set of trade-offs. Key questions remain unresolved: Can consumers meaningfully consent to algorithmic pricing models driven by behavioral data? Are existing transparency and consent mechanisms sufficient? And how can regulators strike a balance between fostering innovation and mitigating harms?

As surveillance pricing practices continue to evolve, particularly with the rapid technological change we have seen in recent years, empirical evidence will be essential to guide policy responses. Future research should aim to measure the real-world impact of these models on consumer welfare, competitive dynamics, and equity. Likewise, any regulatory interventions will need to be carefully calibrated — ensuring consumer protection while preserving the benefits that personalization and data-driven innovation can offer.

50 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union, L 119/1, 4 May 2016, Articles 13–22. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. ("Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles.")

51 Zihao Li, *Affinity-Based Algorithmic Pricing: A Dilemma for EU Data Protection Law*, COMPUTER LAW & SECURITY REVIEW, 46 (2022). See also, Frederik Zuiderveen Borgesius & Joost Poort, *Online Price Discrimination and EU Data Privacy Law*, JOURNAL OF CONSUMER POLICY, 40, 347–366 (2017).

52 Zihao Li, *Regulating Online Algorithmic Pricing: A Comparative Study of Privacy and Data Protection Laws in the EU and US (TTLF Working Paper No. 114)*, STANFORD-VIENNA TRANSATLANTIC TECHNOLOGY LAW FORUM (2024), https://law.stanford.edu/publications/no-114-regulating-online-algorithmic-pricing-a-comparative-study-of-privacy-and-data-protection-laws-in-the-eu-and-us/.

53 Haggai Porat, *Bargaining With Algorithms: An Experiment on Algorithmic Price Discrimination and Consumer and Data Protection Laws (SSRN Working Paper No. 5235056)*, SOCIAL SCIENCE RESEARCH NETWORK (2025).

CPI COMPETITION POLICY® INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.