epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

AND FOUR ORGANIZATIONS

to the

FEDERAL TRADE COMMISSION

Re: Proposed Enforcement Policy Statement Regarding Personalized Pricing

Docket No. FTC-2026-1057

September 25, 2026

The Electronic Privacy Information Center (EPIC) and the undersigned organizations submit these comments in response to the Federal Trade Commission's (FTC or Commission) Proposed Enforcement Policy Statement Regarding Personalized Pricing (Statement).[1]

EPIC is an independent, nonpartisan public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. For decades, EPIC has worked under different administrations to safeguard individuals' personal data and to protect consumer privacy. EPIC focuses public attention on emerging consumer privacy issues, including the use of consumers' personal information in ways that consumers do not expect and that harm them through things such as unfair or discriminatory pricing practices.

[1] Federal Trade Commission's Proposed Enforcement Policy Statement Regarding Personalized Pricing, Fed. Trade Comm'n. (Aug. 19, 2026), https://www.ftc.gov/system/files/ftc_gov/pdf/p034101-ftc-enforcement-policy-statement-re-personalized-pricing-proposed-for-public-comment.pdf [hereinafter "Statement"].

In February 2026, EPIC, along with fourteen other consumer groups, wrote a letter to the FTC, recommending that the FTC promulgate rules requiring companies to disclose the use of surveillance pricing technology.[2] EPIC commends the Commission for taking action on this issue and agrees that consumers deserve to know when a price has been determined using their personal information. The FTC's Statement outlines a comprehensive disclosure, one that will give consumers meaningful information about the types of data being used to set prices. However, based on both extensive expertise in limiting privacy harms and specific policy developments over the past year, EPIC believes that disclosure alone is not enough to adequately protect consumers from surveillance pricing[3] in many instances. The Commission should clarify in its proposed enforcement policy statement that even many disclosed instances of surveillance pricing constitute an unfair practice, and it should consider using its Section 18 authority to promulgate a rule banning the practice.

A growing body of consumer polling, state legislative action, and the FTC's own past actions on unfair data practices all point to the same conclusion: surveillance pricing causes substantial, unavoidable consumer harm that transparency alone cannot cure. The Commission should not lag behind a regulatory landscape that has moved decisively in this direction. States

---

[2] Consumer & Law Student Groups, Comment on Petition for Rulemaking of Andrew Gonzalez Re: Disclosure of Artificial Intelligence Systems for Commercial Profiling and Price Manipulation (Feb. 23, 2026), https://epic.org/wp-content/uploads/2026/02/Consumer-and-Law-Student-Groups_Personalized-Algorithmic-Pricing-Public-Comment_2-23-26.pdf.

[3] EPIC uses "surveillance pricing" throughout these comments rather than "personalized pricing." Both terms describe the same practice of setting the price shown to a consumer based on an analysis of that consumer's personal data and an estimate of what they can be induced to pay. However, "personalized" implies a benefit to the consumer, a benefit that surveillance pricing does not reliably deliver. "Personalized" pricing can also imply that a price is unique to a consumer, whereas in reality the practice it describes can group consumers in segments in which people within a segment see the same price. "Surveillance pricing" on the other hand, describes the mechanism of data-gathering through monitoring a consumer's behavior (e.g. browsing activity, location, purchase history) *see Explaining Surveillance Pricing and Other Data-Driven Pricing Practices*, EPIC & Consumer Federation of America (Aug. 2026), https://epic.org/wp-content/uploads/2026/08/explaining-surveillance-pricing-2026.pdf.

and localities, consumers, and advocacy groups like EPIC are deeply concerned about the affordability and privacy harms of surveillance pricing that cannot be fully ameliorated by transparency. The FTC should be too.

EPIC recommends that the Commission update its Proposed Enforcement Policy to reflect that surveillance pricing constitutes an unfair practice under Section 5 of the FTC Act, and use its rulemaking and enforcement authority to prohibit surveillance pricing practices that cause substantial, unavoidable consumer harm rather than limit its response to disclosure-based remedies.

I. Surveillance pricing is an unfair practice under the FTC's three-part test.

The Commission should expand its Statement or promulgate a rulemaking to clarify that surveillance pricing is an unfair practice, whether or not it is disclosed. Section 5 of the FTC Act provides that an act or practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[4] Surveillance pricing satisfies each element of this test.

A. Surveillance pricing causes substantial injury to consumers.

Surveillance pricing inflicts two distinct but related categories of harms on consumers: pricing harms and privacy harms.

1. Pricing Harms

Surveillance pricing inflicts pricing harm by charging consumers higher prices and by depriving them of the basic informational infrastructure that a well-functioning market requires. As the Statement noted, surveillance pricing depends on setting prices at or near each

[4] 15 U.S.C. § 45(n).

consumer's individual willingness to pay rather than charging a single, transparent price to every customer.[5] Common sense and research both support the intuition that this is likely to raise prices. Many companies are investing large amounts of money into their pricing technologies, and it is unlikely they would be investing this heavily just to make less profit through lowering prices. As the Statement notes, research shows that companies using surveillance pricing are likely to extract more money from consumers, and the more sophisticated they become at these activities, the less benefit to the consumer.[6] By one estimate, surveillance pricing could lead to $1,800 in increased annual household spending.[7] This increased spending is "not a rounding error in a household's budget. The harm is not hypothetical."[8] To the extent that surveillance pricing leads to greater profits through increased market share rather than increasing prices, that effect is likely to be transitory. Consumers will eventually see higher prices as companies using surveillance pricing either consolidate market power, or as more competitors within an industry begin using surveillance pricing. Looking at an isolated transaction may not reflect surveillance pricing's effect on prices cleanly, as the price set by a surveillance pricing algorithm could be higher or lower than a standard market price for any individual consumer at any given moment.

[5] Statement at 3–4.
[6] *Id.*
[7] MIT Digital Fellow Robert Hedges used data from the Bureau of Labor Statistics' Consumer Expenditure Survey and considered the expenditure in categories where surveillance pricing is deployed: groceries, home food delivery, restaurants; apparel and services; household furnishings, supplies, and operation; transportation; entertainment; and personal care. The $1,800 number was calculated based on prior research on price increases applied through surveillance pricing. *Your Data, Their Profit: The Consumer Cost of AI Surveillance Pricing Before the Subcomm. on Crime and Counterterrorism, Comm. on the Judiciary*, 119th Cong. (2026) (statement of Robert Hedges, MIT Digital Fellow, at 16-17) https://www.judiciary.senate.gov/imo/media/doc/a679c902-027a-0e5f-95a4-ac7f0d7a4105/2026-08-04-PM_Testimony_Hedges_bede8206-2a3b-4767-a95d-726b26c178cb2.pdf.
[8] *Id.* at 17.

Overall, however, this practice extracts consumers' money, allowing businesses to capture consumer surplus that would otherwise stay with the consumer.[9]

This extraction is especially troubling because an individual's willingness to pay is not the same as their *ability* to pay. People are generally more willing to pay when they are more desperate, have fewer options to choose from, or are placed in other vulnerable positions. This means that businesses using surveillance pricing may infer that consumers of lower income or those living in majority-minority areas have higher willingness to pay, unfairly charging more for everyday products. For example, neighborhoods with few competing grocery options (also known as "food deserts") are often disproportionately filled with more low-income and greater proportions of non-white residents. People in these neighborhoods have far fewer choices for where to purchase groceries, which often forces consumers to order groceries online. If a surveillance pricing algorithm detects that someone lives in a food desert, infers that they are more willing to pay for online groceries for this reason, and uses this inference to raise prices, the result would be an unfair burden on people likely to be more low-income or from a racially marginalized group.

The Statement's list of examples showcases other concerning potential outcomes of changing price based on individual willingness-to-pay: people with disabilities that are less likely or unable to leave their homes facing higher food delivery prices, people with children facing higher milk prices, people traveling for a funeral facing higher hotel prices, and more.[10] Threatening people who have few or no options with higher prices is fundamentally unfair.

---

[9] *See* David Dayen, *The Emerging Danger of Surveillance Pricing*, Jacobin (July 9, 2024), https://jacobin.com/2024/07/surveillance-personalized-pricing-data-collection ("[P]ersonalized pricing is a transfer of wealth from consumer to the seller. Writ large, the goal and endgame is to maximize revenue.") (quoting Lee Hepner).
[10] Statement at 7–8.

Surveillance pricing also impairs consumers' ability to comparison shop. Comparison shopping is one of the fundamental assumptions underlying the idea of market competition. When prices are set by an opaque, individualized algorithm rather than published at the uniform market rate, consumers cannot determine whether the price they are being charged is fair, let alone if it is the same price charged to everyone else. The erosion of price comparison signals the degradation of a basic market mechanism that lets consumers reward the best deal available. Obscuring price signals also worsens the ever-growing informational asymmetry problems that make surveillance pricing possible.[11] A consumer attempting to compare prices across sellers may find that the price has changed before they finish looking, making the comparison process much more arduous. Imagine that one consumer sees a price of $10, another sees a price of $5, a third sees a price of $7, and a fourth sees the price as $10 with an individualized discount of $3 off. These prices change quickly due to re-calculations of individual willingness to pay and/or the presence of dynamic pricing. How then would any consumer know the true price of a good with which they can comparison shop? They never learn what the price could have been without surveillance, cannot see what anyone else was offered, nor can they bargain over the data used to set the price. This extreme variation in price is not typical of a competitive market. Instead, it reflects a pricing system built to extract a consumer's maximum individual willingness to pay. As described in Section II, a disclosure does not cure the harm caused by surveillance pricing when consumers do not have reliable alternatives to turn to, even once they know a price was personalized.

[11] Stephanie T. Nguyen and Shaoul Sussman, *The Degradation of Prices: Platform Power, the Erosion of Price Comparison, and Rebuilding Comparison Shopping in the Digital Economy*, 56 Seton Hall L. Rev. 1663, 1676 (2026) ("information asymmetry that has fueled retailer price exploitation for the last few decades").

The FTC's own Junk Fees Rule,[12] which is estimated to save consumers up to 53 million hours per year of wasted time and more than $11 billion over the next decade, already establishes that certain types of pricing opacity are independently actionable as unfair or deceptive, regardless of whether the underlying price is reasonable.[13] In adopting that rule, the FTC found that consumers' ability to comparison shop is central to a functioning market and that when businesses obscure the true price, consumers end up paying more and buying more than they would have without the obfuscation. If price opacity from such hidden and misleading fees is already deemed unfair, then price opacity from an individualized algorithm should be deemed unfair for the same reasons.

2. Privacy Harms

Surveillance pricing stems from and contributes to underlying privacy harms. Granular consumer profiling enables surveillance pricing, while surveillance pricing exploits the surveillance of consumers for profit. The result is that companies are financially incentivized to collect more data about consumers, retain it longer, and use it in a way consumers do not expect or welcome: estimating what they can be made to pay. Every additional data point a company collects, from an item left unpurchased in the shopping cart to a change in browsing patterns, becomes an additional input for an individualized price—precisely the kind of use that makes consumers feel that they have lost control over their own information. While companies have been collecting consumer information long before the age of the internet, the data they collect has evolved from rudimentary lists of names and addresses to increasingly granular information

---

[12] 16 C.F.R. §§ 464.2-464.3

[13] *See* Press Release, Fed. Trade Comm'n, FTC Announces Bipartisan Rule Banning Junk Ticket and Hotel Fees (Dec. 17, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/federal-trade-commission-announces-bipartisan-rule-banning-junk-ticket-hotel-fees.

like a consumer's live geolocation to the number of seconds they spend on a product page.[14] It is this granularity that makes the practice of surveillance pricing an alarming progression of modern privacy harms.

The absence of a comprehensive federal privacy law leaves consumers with few tools to push back against this unrestricted data collection and unexpected, harmful uses. Only three states have passed laws directly banning surveillance pricing: Maryland, Connecticut, and New Jersey.[15] Twenty-three states have their own comprehensive privacy laws, but only California and Maryland impose data minimization requirements meaningful enough to seriously limit what data a company can collect and retain for pricing purposes.[16] Elsewhere, state privacy laws do not explicitly prevent companies from collecting and using consumer data for pricing so long as they disclose that use in their privacy policies. Individuals should have the ability to control access to information about themselves, how it is used, or to whom it is disclosed.[17] Intuitions about privacy support this: a person may tell a friend something personal without authorizing that information to be disclosed to their employer.[18] Corporate data practices today take that control away. Given that the average consumer does not read privacy policies, or have the ability to change their terms even if they did, consumers cannot give meaningful and informed consent, especially when they are unaware of the extent of the data being collected and disclosed and

---

[14] *See* Press Release, Fed. Trade Comm'n, FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices (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-consume (finding that a wide range of personal data is used to set prices, from demographic and location data to mouse movements).
[15] S.B. 4, 2026 Gen. Assemb., Reg. Sess. (Conn. 2026); H.B. 895, 449th Gen. Assemb., Reg. Sess. (Md. 2026); A. 4523, 222nd Leg., Reg. Sess. (N.J. 2026).
[16] *See* Caitriona Fitzgerald & Kara Williams, *The State of Privacy: How State "Privacy" laws Fail to Protect Privacy and What They Can Do Better*, EPIC 5 (Jan. 2025) https://epic.org/documents/the-state-of-privacy-2025-how-state-privacy-laws-fail-to-protect-privacy-and-what-they-can-do-better/ (giving only California and Maryland a "B" grade for their privacy laws).
[17] Daniel J. Solove, *Understanding Privacy*, Harv. Univ. Press 18-21, 24-29 (2008).
[18] Julie E. Cohen, *What is Privacy For*, 126 Harv. L. Rev. 1904, 1908 (2013).

when alternatives are limited or outright unavailable.[19] They acquiesce, not because they intend for their data to be processed, but because they do not have any other options and feel powerless about their privacy rights.[20] Companies' ability to aggregate data across sources compounds this loss of control because aggregation "reveals facts about data subjects in ways far beyond anything they expected when they gave out the data."[21]

What makes surveillance pricing distinctively harmful is not just the data companies collect, but what they can infer from it. The same data infrastructure that makes surveillance pricing possible enables companies to build hyper-specific behavioral profiles that can not only identify a consumer but also their state of mind while making purchases.[22] The FTC's 6(b) Staff Perspective explained that these algorithms could deliberately target reluctant gamblers and encourage impulse shopping from homeowners living in areas affected by flooding or other critical emergencies.[23] Surveillance pricing is most profitable precisely when it can identify a consumer who is most vulnerable, most pressed for time, most geographically constrained, or most emotionally compromised and price accordingly. That is what distinguishes it from ordinary market pricing, which responds to supply and demand, and from the conventional discounting practices that involve a greater amount of transparency and consumer choice. While prohibiting surveillance pricing will not, on its own, address the root causes of these broader

---

[19] Colleen McClain et al., *How Americans View Data Privacy*, Pew Research Ctr. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ ("More than half of Americans (56%) say they always, almost always or often click 'agree' without reading privacy policies.").
[20] Solove, *supra* note 17, at 132.
[21] *Id.* at 119.
[22] Robert G. Reeve (@RobertGReeve), X (May 24, 2021, at 23:32 ET) https://x.com/RobertGReeve/status/1397032784703655938.
[23] Fed. Trade Comm'n, *FTC Surveillance Pricing 6(b) Study: Research Summaries, A Staff Perspective* 6 (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf

privacy harms, it will prevent corporations from deploying unfair data extraction practices at the expense of consumers.

The Commission has previously enforced Section 5 against companies engaging in similar privacy-invasive practices. For example, it has banned data brokers from selling and using sensitive location data.[24] Notably, it required these companies to cease the practices altogether, not merely to disclose the practices to consumers.

B. Surveillance pricing injuries are not reasonably avoidable.

Consumers have few meaningful ways to avoid surveillance pricing. First, the sectors where surveillance pricing is most commonly deployed center on essential goods and services—groceries, food delivery, household items, healthcare, transportation, and housing—where consumers cannot simply decline to participate in the market. E-commerce, where surveillance pricing is easiest to achieve, accounts for a steadily increasing share of all shopping (17.1% in the second quarter of 2026, up from 15.5% a year before).[25] Roughly 87% of American consumers shop online, and retail e-commerce sales are projected to grow at a compound annual rate of 6% through 2030,[26] so it is not reasonable to expect consumers to avoid online shopping altogether to escape a pricing practice they may not even know is occurring.

Second, surveillance pricing is not confined to a handful of outlier companies. The FTC's 6(b) study found that the seven companies it examined that provided such pricing solutions

---

[24] *See* Fed. Trade Comm'n, Press Release, *FTC to Ban Kochava and Subsidiary from Selling Sensitive Location Data to Settle Charges They Sold Location Data Linked to Millions of Mobile Devices* (May 4, 2026) (explaining a ban on selling sensitive location data); Federal Trade Commission, Press Release, *FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites* (Dec. 3, 2024) (prohibiting the sale or use of sensitive location data).
[25] U.S. Census Bureau News, Quarterly Retail E-Commerce Sales, 2nd Quarter (Aug. 18, 2026), https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.
[26] *Online Shopping Behavior in the United States - Statistics & Facts*, Statista (Aug. 13, 2026). https://www.statista.com/topics/2477/online-shopping-behavior/.

served at least 250 clients across a range of industries, meaning consumers often cannot "shop around" to avoid surveillance pricing simply by switching sellers within the same category.[27] This is especially true in industries that have consolidated, such as grocery. And since the Commission conducted the study throughout 2024, those data are now a likely under-count.

Third, consumers cannot avoid what they cannot identify. Surveillance pricing is, by design, opaque. Consumers typically do not know which of the companies they patronize use it, what data feeds it, or how a specific price was generated. A consumer cannot negotiate with a seller, benchmark an offered price against an objective market rate, or decline a service altogether when they do not know the practice is happening in the first place.

C. Surveillance pricing injuries are not outweighed by countervailing benefits.

Proponents of surveillance pricing typically offer three benefits to justify the practice: (1) economic efficiency gains, (2) providing targeted discounts, and (3) operationalizing a kind of progressive pricing scheme by charging more to buyers who can afford to pay more and less to those who cannot. None of these justifications withstands scrutiny or outweighs the substantial injury described above.

First, surveillance pricing does not produce efficiency gains that truly benefit consumers. Proponents argue that individualized pricing improves market efficiency because a seller can expand the market and reduce wasted surplus by selling to more consumers at their precise willingness to pay. But as the Commission's Statement described, as surveillance pricing becomes more precise, net consumer welfare will likely fall.[28] The output expansion that

[27] Fed. Trade Comm'n, *FTC Surveillance Pricing 6(b) Study: Research Summaries, A Staff Perspective* (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf.
[28] Statement at 3–4.

companies predict is speculative, whereas the extraction of consumer surplus is the stated design goal. And, as the research shows, any benefits to some consumers are accompanied by losses to others.[29] The consumers who "lose" in this scenario are likely to be members of vulnerable groups who, for various reasons, may display a higher individual willingness to pay. In these situations, a firm's pricing exploits a structural advantage rather than reflecting legitimate costs or competitive dynamics.

Second, surveillance pricing cannot be justified as a good-faith effort to extend more discounts and expand access to consumers who would not have otherwise purchased at full price. Marketing materials for surveillance pricing tools routinely tell prospective business customers that offering the same discount to every customer leaves money on the table.[30] These tools now leverage AI to help determine "the optimal incentive level for each customer, avoiding over-discounting customers who would have purchased anyway."[31] That pitch confirms that the real purpose of the practice is not to identify who most needs a lower price but to identify who can be charged the most.

Third, surveillance pricing does not function as a progressive pricing scheme. A genuinely progressive pricing scheme would require some judgment about need or ability to pay. Surveillance pricing instead optimizes for individual willingness to pay, in a manner designed to maximally turn consumer surplus (the difference between what the shopper would have been willing to pay and what the shopper actually paid) into seller profit across all shoppers. If anything, surveillance pricing risks compounding existing inequities rather than correcting them.

---

[29] *Id.* at 4.
[30] Tepia, *Plexure and McDonald's: Revolutionizing Personalized Experiences*, https://tepia.co/plexure-and-mcdonalds-revolutionizing-personalized-experiences/ (last visited Sept. 20, 2026).
[31] Eagle Eye, *AI Personalized Promotions for Retail*, https://eagleeye.com/personalized-promotions (last visited Sept. 20, 2026).

Research on consumer markets has long documented a "poverty penalty": lower-income consumers and consumers of color often pay more for comparable goods and services, in part because of discriminatory pricing in markets such as auto sales and insurance.[32] A pricing system that further optimizes around what a given consumer can be made to pay exploits that existing disparity.

The intent of highlighting these harms is not to question discounts based on observable, publicly disclosed characteristics that a consumer can affirmatively opt into, such as a student or senior discount upon presenting a valid ID. EPIC has previously noted in its state advocacy work that “transparent and uniformly offered discounts” like student discounts or happy hours do not require covert collection and retention of behavioral data to administer and thus should be excluded from any restrictions on surveillance pricing.[33] What distinguishes surveillance pricing is not that it involves differential pricing at all, but that it is built on the collection and retention of behavioral data the consumer did not choose to share rather than a characteristic a consumer voluntarily discloses in exchange for a defined, transparent benefit. EPIC believes that the Commission’s rulemaking process is the appropriate venue to work out precisely where that line falls.

[32] *See* Julia Angwin, Jeff Larson, Lauren Kirchner & Surya Mattu, *Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk*, ProPublica (Apr. 5, 2017), https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk; Ian Ayres & Peter Siegelman, *Race and Gender Discrimination in Bargaining for a New Car*, 85 Am. Econ. Rev. 304 (1995).

[33] EPIC, *Testimony in Support of A 4085, the Fair Price Protection Act*, N.J. Gen. Assembly, Assembly Commerce & Econ. Dev. Comm. (May 2026), https://epic.org/documents/new-jersey-testimony-in-support-of-a-4085-the-fair-price-protection-act/.

II. A transparency-only approach does not address many of surveillance pricing's underlying harms and does not reflect consumer preferences, legislative developments, or privacy law best practices.

A transparency-only approach to combating surveillance pricing is unlikely to be effective and would lag behind bipartisan consumer preference and regulatory consensus. In August 2026, at the Senate Judiciary Committee's hearing on surveillance pricing, Senator Josh Hawley was unequivocal in his characterization of surveillance pricing, calling it the "unholy trinity of everything Americans hate: spying on people, ripping them off, and taking away jobs."[34] The FTC has a unique opportunity to promulgate rules that will find support among a broad swath of American consumers and to provide businesses of all sizes a clear, fair baseline while supporting the efforts of state legislatures and attorneys general.

A. Transparency alone cannot remedy many surveillance pricing harms.

Surveillance pricing imposes widespread harms to affordability and privacy, very few of which can be remedied by a transparency-only approach. Disclosures are only a meaningful remedy for a consumer who can act on the information received, but that is not often the case with surveillance pricing. Consumers have few real exits from surveillance pricing due to the practice's presence throughout the economy and the consolidation seen in many markets. For instance, "[a] wave of sustained consolidation is sweeping through regional grocery chains across the United States."[35] Based on disclosures in compliance with the New York Algorithmic

---

[34] *Your Data, Their Profit: The Consumer Cost of AI Surveillance Pricing Before the Subcomm. on Crime and Counterterrorism, Comm. on the Judiciary*, 119th Cong., at 26:37-26:46 (2026) (statement of Sen. Josh Hawley, Chairman, S. Comm. on Crime and Counterterrorism), https://www.judiciary.senate.gov/committee-activity/hearings/your-data-their-profit-the-consumer-cost-of-ai-surveillance-pricing.

[35] Mike Ross & Jeffrey Coseo, *Is Consolidation Quietly Coming for Your Neighborhood Grocery Store?*, Price Waterhouse Cooper (June 17, 2026), https://www.pwc.com/us/en/industries/consumer-markets/grocery-deals-consolidation-outlook.html; *see also* Stacy Mitchell & Kate Milani, *How Corporate Consolidation Broke America's Grocery System*, Institute for Local Self-Reliance (Jan. 28, 2026), https://ilsr.org/wp-content/uploads/2026/01/ILSRGroceryConsolidationIssueBrief.pdf.

Pricing Disclosure Act, Aldi, Target, Food Bazaar, and Instacart all set prices using personal data. Analyzing their privacy policies, patent applications, and consumer segmentation activities shows that it is highly likely that Kroger and Walmart have also implemented surveillance pricing, though the companies deny the claim.[36] The same applies in other sectors: both Lyft and Uber seem to engage in surveillance pricing, as do UberEats, Grubhub, Postmates, DoorDash and Seamless, though many of these companies also deny the claim.[37] These companies represent a large percentage of their respective markets.[38] Informing consumers in these

[36] In an investigation, Consumer Reports found that Kroger develops extensive profiles of its consumers and that Kroger offers personalized discounts based on purchase data and "demographic or online behavioral data." Derek Kravitz, *Inside Kroger's Secret Shopper Profiles: Why You May Be Paying More Than Your Neighbors*, Consumer Reports (May. 21, 2025), https://www.consumerreports.org/money/questionable-business-practices/kroger-secret-grocery-shopper-loyalty-profiles-unfair-a1011215563/. In describing the purposes for which Walmart uses consumer data, Walmart's privacy policy states: "we may also use [personal information] to provide you with a more personalized Walmart experience, including to improve and deliver tailored online ads, product recommendations, and **promotions**" (emphasis added). Walmart Customer Privacy Notice (Online and In-Store), Walmart (Aug. 20, 2026), https://corporate.walmart.com/privacy-security/walmart-privacy-notice. *See also* Christopher Yang, *What Walmart's AI Pricing Patents Mean for Every Retailer*, Inc. (May. 27, 2026), https://www.inc.com/christopher-yang/what-walmarts-ai-pricing-patents-mean-for-every-retailer/91350049 (descripting two patents Walmart obtained in January and March 2026, "designed to dynamically and automatically update item prices using predicted demand and consumers' price sensitivity" and "a machine-learning system that forecasts demand and recommends prices using data sources such as pervious purchases, prices, methods of payment, and customer identification" respectively).

[37] Alex Bitter, *Uber and DoorDash Now Disclose When Algorithms Set Prices. There's Still One Big Question.*, Business Insider (Nov. 12, 2025), https://www.businessinsider.com/uber-doordash-notify-if-apps-use-customer-data-set-prices-2025-11.

[38] Aliza Vigderman, *2026 Rideshare Statistics*, Autoinsurance (last updated May 6, 2026), https://www.autoinsurance.com/research/rideshare-statistics/ (reporting that in March 2024, Uber and Lyft held 76% and 24% of U.S. rideshare market). Depending on the location, only two or three grocery stores can control a large share of the market. For example, in Santa Fe, New Mexico, Kroger and Albertsons together make up 59% of the market share. American Economic Liberties Project, Press Release, FTC Previews Hard Evidence of Harms While Kroger and Albertsons Dangle Unenforceable Promises in Merger Hearing Opening Arguments (Aug. 27, 2024), https://www.economicliberties.us/press-release/ftc-previews-hard-evidence-of-harms-while-kroger-and-albertsons-dangle-unenforceable-promises-in-merger-hearing-opening-arguments/.

industries of surveillance pricing practices does little to ameliorate the harms they face because there are not reliable alternatives for customers to turn to.[39]

The Statement's own scenarios demonstrate the limited remedial effect of a transparency-only approach. Consider the first example: "A food delivery company quoting a higher price to consumers on the basis of data personal to those consumers that lead the company to believe they are less likely or unable to leave their homes to purchase food."[40] Imagine a consumer with mobility difficulties that make it difficult to leave home to grocery shop or pick up food. What, armed with a disclosure, can this consumer do? Selecting a competitor is unlikely to help given that many food delivery companies seem to be engaging in or experimenting with surveillance pricing. This consumer would likely prefer that the practice be banned. Charging people more because a disability limits their options runs contrary to the principle of equal participation in the marketplace that animates the Americans with Disabilities Act.

A transparency-only approach does not return the data that was collected, provide a benchmark price to compare against, or change the reality that the consumer has no practical way to act on the disclosure once it is made. As the next Part will show, the majority of surveillance pricing bills ban the practice and deem violations to be an unfair and deceptive practice.

---

[39] *See* Patrick K. Lin, *Surveillance Pricing: Exploiting Informational Asymmetries*, LPE Blog (Apr. 20, 2026), https://lpeproject.org/blog/surveillance-pricing-exploiting-information-asymmetries/ ("[I]ndividuals often lack the necessary expertise or resources to make sense of disclosed information, resulting in information overload or fatigue… The disclosure approach is untenable as digital products and services become increasingly essential for navigating daily life."); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1487 (2019) (criticizing the idea of voluntary consent when choosing an Internet Service Provider saying, "[T]o 'choose' not to use the Internet is in a very real sense to 'choose' not to participate in modern society or the modern economy. This might not quite be 'sign or die,' but it's close to 'sign or not live like most people.'").

[40] Fed. Trade Comm'n, Proposed Enforcement Policy Statement Regarding Personalized Pricing 7 (Aug. 19, 2026), https://www.ftc.gov/system/files/ftc_gov/pdf/p034101-ftc-enforcement-policy-statement-re-personalized-pricing-proposed-for-public-comment.pdf.

B. The public supports bans on surveillance pricing, and lawmakers have begun delivering.

The public's awareness of and opposition to surveillance pricing has grown over the past year. According to a recent survey of 1,000 voters, GBAO Strategies, a public opinion research firm, found that 68% of voters believe that surveillance pricing would lead to an increase in grocery prices.[41] Seventy-five percent believe that surveillance pricing will lead to consumers being charged more than they can afford. Voters are uncomfortable with their data being used to set prices. Another study, conducted by Groundwork Collaborative, found that 76% of people believe that using personal information about customers to charge different consumers different prices for the same product is unfair.[42] Even when asked how they felt about personal data being used to offer consumers a discount, 64% maintained that they viewed the practice as unfair.[43] In the same study 73% of consumers said they believed that companies benefited more than customers when they used personal data to set personalized prices.[44] An overwhelming majority, 73%, also supported banning the use of personal data for pricing.[45]

In an April 2026 study by Lake Research Partners and the American Economic Liberties Project, focus group participants arrived with little to no awareness of surveillance pricing but

---

[41] Polling Memorandum from GBAO Strategies to Interested Parties, Voters Say No to Digital Price Tags & Surveillance Pricing (May 26, 2026), https://www.ufcw.org/wp-content/blogs.dir/61/files/2026/05/GBAO-UFCW-National-Survey-Memo-052626.pdf [hereinafter GBAO Memorandum].
[42] Groundwork Collaborative & Data for Progress, Strong Majority of Americans Want Corporations to End Deceptive Surveillance Pricing Schemes 13 (May 21, 2026), https://www.filesforprogress.org/datasets/2026/5/dfp-gwc-dynamic-pricing-crosstabs.pdf.
[43] *Id.* at 14.
[44] *Id.* at 22.
[45] Other surveys highlight the same trends in consumer sentiment. In a poll of 541 likely New York voters, 70% supported New York's ban on surveillance pricing. Groundwork Collaborative & Data for Progress, Groundwork Celebrates Passage of New York's One Fair Price Act 5 (May 2026), https://www.filesforprogress.org/datasets/2026/5/dfp_gwc_nys_surveillance_pricing_ffp_topline.pdf. *See also* GBAO Memorandum, *supra* note 41 (finding "strong bipartisan support for banning" digital price tags and surveillance pricing).

left the sessions "passionately opposing the practice and with a strong desire for Congress to take immediate action to ban surveillance pricing."[46] The study found that a vast majority of participants believed that "corporations and their CEOs would benefit the most from surveillance pricing."[47] The study found that opposition to surveillance pricing is bipartisan, with participants across age groups and political affiliations describing the practice using terms like "discriminatory," "manipulative," and "price gouging."[48] When asked about how they would most effectively regulate surveillance pricing, a vast majority expressed preference for a nationwide ban.[49] When presented with the choice between an opt-out disclosure regime and an outright ban, the clear preference was for prohibition since an opt-out right would be meaningless in practice given "how many lengthy terms and conditions are hidden on every website and how companies will use language to make surveillance pricing sound innocuous."[50]

The public outcry over surveillance pricing has driven an impressive regulatory response. Since the beginning of 2026, 28 states have introduced at least 48 bills that regulate surveillance pricing. Thirty-seven out of the 48 introduced bills prohibit surveillance pricing.[51] Earlier this year, Connecticut, Maryland, and New Jersey enacted legislation banning surveillance pricing in grocery and food delivery sectors in their respective states.[52] The Connecticut and Maryland bans will go into effect on October 1, 2026, while the New Jersey bans will go into effect on July 1,

---

[46] Memorandum from Lake Research Partners to American Economic Liberties Project, Key Findings from Focus Groups on Surveillance Pricing (Apr. 3, 2026), https://www.economicliberties.us/wp-content/uploads/2026/05/LRP-AELP-Focus-Group-Memo-f-4.27.2026.pdf.
[47] *Id.* at 13.
[48] *Id.* at 1.
[49] *Id.* at 2-3.
[50] *Id.* at 10.
[51] Relatedly, since the beginning of 2026, 15 states have introduced at least 28 bills regulating algorithmic rent setting. *See, e.g.*, Heather Vogell, *Rent Going Up? One Company's Algorithm Could Be Why*, ProPublica (Oct. 15, 2022), https://www.propublica.org/article/yieldstar-rent-increase-realpage-rent.
[52] S.B. 4, 2026 Gen. Assemb., Reg. Sess. (Conn. 2026); H.B. 895, 449th Gen. Assemb., Reg. Sess. (Md. 2026); A. 4523, 222nd Leg., Reg. Sess. (N.J. 2026).

2027. A New York bill banning surveillance pricing is awaiting Gov. Hochul's signature.[53] Notably, the New York Legislature felt the need to pass a bill banning surveillance pricing less than a year after the disclosure requirement went into effect in the state, indicating an acknowledgement that a disclosure-only regime was insufficient.[54]

At the federal level, Representative Greg Casar introduced the Stop AI Price Gouging and Wage Fixing Act, which would ban companies from using automated decision systems that use personal information to set prices or determine wages.[55] In the Senate, Senator Ruben Gallego introduced the One Fair Price Act, prohibiting the use of surveillance pricing. The bill declares it "unlawful" for a person "to offer or charge different consumers for the same or a substantially similar product or service, using, informed by, or based on, in whole or in part, surveillance pricing."[56]

Lawmakers have also begun investigations of surveillance pricing practices. In March 2026, the House Oversight Committee sent letters to Lyft, Uber, Expedia, Instacart, and Booking.com requesting documents describing the revenue management platforms used by the companies, the utilization and applications of consumer data, the organizations from whom data is bought and with whom it is disclosed, and the mechanism through which consumer data determines prices.[57] In May 2026, Representative Frank Pallone, Jr. launched a Congressional inquiry into surveillance pricing, sending a letter to 25 corporations—all grocery stores, convenience stores, and pharmacies—requesting information on a series of questions about the

---

[53] A. 9349B, 249th Leg., Reg. Sess. (N.Y. 2026).
[54] A. 9349B, 249th Leg., Reg. Sess. (N.Y. 2026).
[55] Stop AI Price Gouging and Wage Fixing Act of 2025, H.R. 4640, 119th Cong. (2025).
[56] One Fair Price Act, S. 3387, 119th Cong. § 2(a)(1) (2025).
[57] Press Release, Representative James Comer, Comer Investigates Use of Artificial Intelligence to Set Prices for Consumers (Mar. 5, 2026), https://oversight.house.gov/release/comer-investigates-use-of-artificial-intelligence-to-set-prices-for-consumers/.

company's data collection and price setting practices.[58] On January 26, 2026, California Attorney General Rob Bonta initiated an investigation of whether companies' surveillance pricing practices violated the California Consumer Privacy Act.[59]

Given the consumer and state legislature response to surveillance pricing, a transparency-only approach to addressing this pricing practice is insufficient. This is also borne out by the myriad disclosure laws that regulate much of modern technology.[60] Despite the ubiquity of disclosures, their efficacy has long been questioned. Consumers do not read disclosures.[61] Disclosures contain large amounts of complex information, leading to cognitive overload.[62] Studies have estimated that consumers would need to spend dozens of hours per month to actually read each privacy policy they agree to while surfing the web.[63]

[58] Press Release, Representative Frank Pallone, Jr., Pallone Launches Surveillance Pricing Inquiry (May 13, 2026), https://pallone.house.gov/media/press-releases/pallone-launches-surveillance-pricing-inquiry.

[59] *See* Rob Bonta, California Attorney General, Press Release, On Data Privacy Day, Attorney General Bonta Focuses on Surveillance Pricing, Compliance with California Consumer Privacy Act (Jan. 27, 2026), https://oag.ca.gov/news/press-releases/data-privacy-day-attorney-general-bonta-focuses-surveillance-pricing-compliance.

[60] Richards & Hartzog, *supra*, note 39, at 1463 ("Consent is the foundation of the relationships we have with search engines, social networks, commercial web sites, and any one of the dozens of other digitally mediated businesses we interact with regularly.").

[61] This is not a criticism of the typical consumer. As Peter M. Tiersma notes, "even highly educated judges may have trouble with consumer documents." Tiersma quotes Chief Justice Weintraub of the New Jersey Supreme Court as admitting, "I don't know what it means. I am stumped," when confronted with an insurance policy. Peter M. Tiersma, *Legal Language*, Univ. of Chi. Press 219 (1999**)**. Chief Justice John Roberts has also admitted to not reading fine print, saying that it has "the smallest type you can imagine and you unfold it like a map." Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, ABA Journal (Oct. 20, 2010), https://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/.

[62] Carl E. Schneider & Omri Ben-Shahar, *More Than You Wanted to Know: The Failure of Mandated Disclosure*, Princeton Univ. Press 8 (2014).

[63] Irma Šlekytė, *NordVPN Study Shows: Nine Hours to Read the Privacy Policies of the 20 Most Visited Websites in the US*, NordVPN.com (Oct. 23, 2023), https://nordvpn.com/blog/privacy-policy-study-us/; Shankar Vedantam, *To Read All Those Web Privacy Policies, Just Take A Month Off Work*, NPR (Apr. 19, 2012), https://www.npr.org/sections/alltechconsidered/2012/04/19/150905465/to-read-all-those-web-privacy-policies-just-take-a-month-off-work.

Additionally, even if companies *could* provide simple disclosures, they often refuse to do so. For example, New York's Algorithmic Pricing Disclosure Act mandates a "clear and conspicuous disclosure" that includes the following statement: "This price was set by an algorithm using your personal data."[64] In response, companies like Instacart have provided the following disclosure: "New York law requires the following disclosure because certain prices and/or fees may vary based on randomized tests, we use personal information (such as delivery address) to calculate fees, and we offer certain personalized incentives: this price was set by an algorithm using your personal data."[65] Instacart provides *more* information than the law requires, and in doing so, raises more questions than it answers. It buries the simple statement the law requires under three vague clauses and creates the exact cognitive overload that causes readers' eyes to glaze over and skip the disclosure.

The guidelines for effective personalized pricing disclosures provided by the FTC are a notable improvement over the disclosure required by the New York Algorithmic Pricing Disclosure Act. For instance, the FTC's proposed recommendation to disclose the basis for personalization and the type of data used provides consumers with more meaningful information than under the New York law. The focus on the accuracy and completeness of disclosures will enable consumers to identify for themselves whether the data being processed for personalization is reasonably related to the cost of providing a service or derived from behavioral characteristics and income estimates that approximate individual willingness to pay.[66]

However, even the FTC's recommended disclosure will face challenges. Companies have been complying with New York's disclosure law by placing disclosures on the bottom of the

---

[64] Algorithmic Pricing Disclosure Act, S. 3008C, 248th Leg., Reg. Sess. § 349-a(2) (N.Y. 2025).
[65] *See* Appendix A.
[66] Statement at 6-7 ("Telling a consumer only that he is being shown a 'specially selected' price, for example, would likely be misleading because it omits important information.").

checkout screen. Whether accessing the company's website on a computer or through a mobile application, consumers are usually able to proceed with a transaction without viewing the disclosure.[67] The challenge of presenting contemporaneous disclosures within the confines of limited screen real estate will persist even with the FTC's disclosure. This issue will be compounded by the comprehensive nature of the FTC's disclosure guideline. Companies often collect various categories of data for pricing purposes,[68] and it is difficult to imagine the volume of text the disclosure will necessitate being presented in a reader-friendly manner given current design of most user interfaces and the presentation of currently mandated disclosures.

III. The FTC has the regulatory authority to ban surveillance pricing.

In its Statement, the FTC asserts that Congress has not given it the authority to prohibit personalized pricing in all circumstances.[69] However, this position ignores the Commission's authority under Section 5 to regulate unfair practices and its authority under Section 18 to promulgate rules against unfair pricing practices. The Commission used its Section 18 authority

[67] When viewing websites on a computer, disclosures are typically placed below the button used to continue the transaction (e.g., Instacart, Aldi) or are hidden behind an "information" icon (e.g., Target). Similarly, when on a mobile application, disclosures are placed at the bottom of the screen. Consumers have to intentionally scroll to the bottom of the screen to view the disclosure. As a result, consumers can complete the transaction without ever encountering the disclosure.

[68] McDonald's privacy policy, for example, states that McDonald's collects the following data from consumers to administer their loyalty program: "[1] Identifiers, such as participants' name, email address, (optional) day and month of birth, and MyMcDonald's Rewards account numbers; [2] Personal information . . . such as phone number and payment information . . . ; [3] Commercial information, such as records of members' purchases, information about actions taken while using the McDonald's app, and members' rewards account credentials; [4] Internet or other electronic network information reflecting a participants' interaction with [McDonald's Application/Rewards Program]; [6] Geolocation data . . .; and [7] Inferences drawn from any of the above categories of information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes." *McDonald's Global Customer Privacy Statement*, McDonald's, https://www.mcdonalds.com/us/en-us/privacy.html (last visited Sept. 17, 2026).

[69] Fed. Trade Comm'n, Proposed Enforcement Policy Statement Regarding Personalized Pricing (Aug. 19, 2026), https://www.ftc.gov/system/files/ftc_gov/pdf/p034101-ftc-enforcement-policy-statement-re-personalized-pricing-proposed-for-public-comment.pdf ("Congress has not given the Commission the authority to prohibit personalized pricing in all circumstances . . .").

when it adopted the Junk Fees Rule, which prohibits a pricing practice the Commission found unfair and deceptive.[70] The Statement's own analysis would support most of what a rule prohibiting surveillance pricing would require.

Section 5(a)(1) of the FTC Act states that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[71] Thus, a wide range of commercial behaviors and activities are well within the Commission's purview. The Commission "does not arrogate excessive power to itself if, in measuring a practice against the elusive but congressionally mandated standard of fairness, it. . . considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws."[72] The FTC can enforce Section 5 in two primary ways. The Commission can bring one case at a time,[73] or it can issue a rule under Section 18 that prohibits a practice.[74]

According to the FTC's own Statement, the agency has already concluded that surveillance pricing is within the reach of Section 5.[75] In the operative section of the Statement, titled "Personalized Pricing Without Adequate Disclosures Likely Violates Section 5," the Commission reaches that conclusion under the deception and unfairness prongs. As discussed in Section I, surveillance pricing satisfies each element of the unfairness test in Section 5(n). The open question, then, is the proper remedy and vehicle.

Beyond revising the Statement, the Commission could also invoke its Section 18 authority to adopt a rule banning surveillance pricing. Section 18 of the FTC Act authorizes the

---

[70] Trade Regulation Rule on Unfair or Deceptive Fees, 90 Fed. Reg. 2066 (Jan. 10, 2025) https://www.federalregister.gov/d/2024-30293 [hereinafter Junk Fees Rule].
[71] 15 U.S.C. § 45(a)(1).
[72] *FTC v. Sperry Hutchinson Co.*, 405 U.S. 233, 244 (1972).
[73] 15 U.S.C. § 45(b).
[74] 15 U.S.C. § 57a(a)(1)(B).
[75] Statement, at 4-6 (Part III).

Commission to prescribe “rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce” within the meaning of Section 5(a)(1) of the Act.[76] Before promulgating such a rule, the Commission must have reason to believe that the unfair practices are “prevalent.”[77] These rules may include “requirements prescribed for the purpose of preventing such acts or practices.”[78] This gives the Commission the authority to wholly prohibit a practice, since a ban is the most direct way to prevent an unfair practice, and once a rule takes effect, violating it is itself an unfair or deceptive act.[79] Congress gave Section 18 its own procedural requirements to craft specific rules to prohibit harmful practices to consumers. Section 18 states that the Commission’s authority to issue rules about unfair or deceptive practices is granted only under this particular section.[80] Therefore, a rule prohibiting surveillance pricing on the basis of unfairness falls under Section 18.

The record already before the Commission satisfies the prevalence standard. Under Section 18(b)(3), prevalence may be shown by 'any other information available to the Commission' indicating a widespread pattern of the practice.[81] The Commission's own 6(b) study found that just seven pricing vendors served at least 250 clients across numerous industries—a figure that, given the study's 2024 timeframe, likely understates current adoption. Disclosures under New York's Algorithmic Pricing Disclosure Act indicate that major grocery retailers and delivery platforms have deployed the practice,[82] and ongoing congressional inquiries span the rideshare, travel, grocery, and pharmacy sectors.

---

[76] *Id.* § 57a(a)(1)(B).
[77] *Id.* § 57a(b)(3).
[78] *Id.* § 57a(a)(1)(B).
[79] *Id.* § 57a(d)(3) (once a rule takes effect, “a subsequent violation thereof shall constitute an unfair or deceptive act or practice in violation of section 45(a)(1)”).
[80] *Id.* § 57a(a)(2).
[81] 15 U.S.C. § 57a(b)(3).
[82] *See* Appendix A.

The Commission's recent Trade Regulation Rule on Unfair or Deceptive Fees, also known as the Junk Fees Rule, demonstrates the viability of this approach.[83] The Junk Fees Rule states that "it is an unfair and deceptive practice" for a business selling live-event tickets or short-term lodging to offer, display, or advertise a price without clearly and conspicuously disclosing the total price, or to misrepresent the nature, purpose, amount, or refundability of any fee.[84] The Commission built the Junk Fees Rule on the premise that the practice was unfair because it frustrated consumers' ability to "shop for price effectively."[85] The Commission noted that industry-standard disclosures were not enough because "piecemeal numbers and explanations cannot cure the deception or mitigate the harms to consumers when businesses employ these pricing tactics."[86] A consumer facing surveillance pricing is in an even worse position than when a consumer is facing junk fees because surveillance pricing erodes the idea of a true price entirely and frustrates a consumer's ability to engage in meaningful price comparisons. Junk fees could be remedied through disclosure of the true, overall price, but surveillance pricing attacks the very idea of a true, overall price. If junk fees are unfair since they frustrate comparison shopping, surveillance pricing is unfair for the same reason and to a greater degree.

IV. Conclusion

EPIC urges the FTC to withdraw its assertion that it lacks authority to prohibit personalized pricing and to declare that surveillance pricing is an unfair practice under Section 5 of the FTC Act rather than merely a practice requiring disclosure. As detailed above, surveillance pricing satisfies each element of the Section 5(n) unfairness test: it causes substantial injury

[83] Junk Fees Rule, 90 Fed. Reg. 2066.
[84] 16 C.F.R. §§ 464.2(a), 464.3 (2025).
[85] 90 Fed. Reg. 2066, 2067.
[86] *Id.*

through inflated prices and the compounding harms of data collection; the injury is not reasonably avoidable by consumers who must purchase groceries, healthcare, and other necessities; and it is not outweighed by any countervailing benefit to consumers or competition. Disclosure does not solve any of these three elements because it does not lower the price charged, does not return the data collected, and does not give consumers a realistic path to act on the information once received. Consumers have made clear through polling, focus groups, and congressional and state testimony that they want this practice stopped, not merely disclosed. The regulatory landscape has already moved decisively in this direction, and the Commission has the authority under Section 5 and Section 18 of the FTC Act to move alongside it. EPIC accordingly recommends that the Commission prohibit surveillance pricing as an unfair practice. If you have any additional questions, please contact Tom McBrien at mcbrien@epic.org and Kara Williams at williams@epic.org.

Sincerely,

Electronic Privacy Information Center
Center for Digital Democracy
Consumer Federation of America
National Consumers League
Demand Progress Education Fund

/s/ Tom McBrien
Counsel
Electronic Privacy Information Center

/s/ Kara Williams
Counsel
Electronic Privacy Information Center

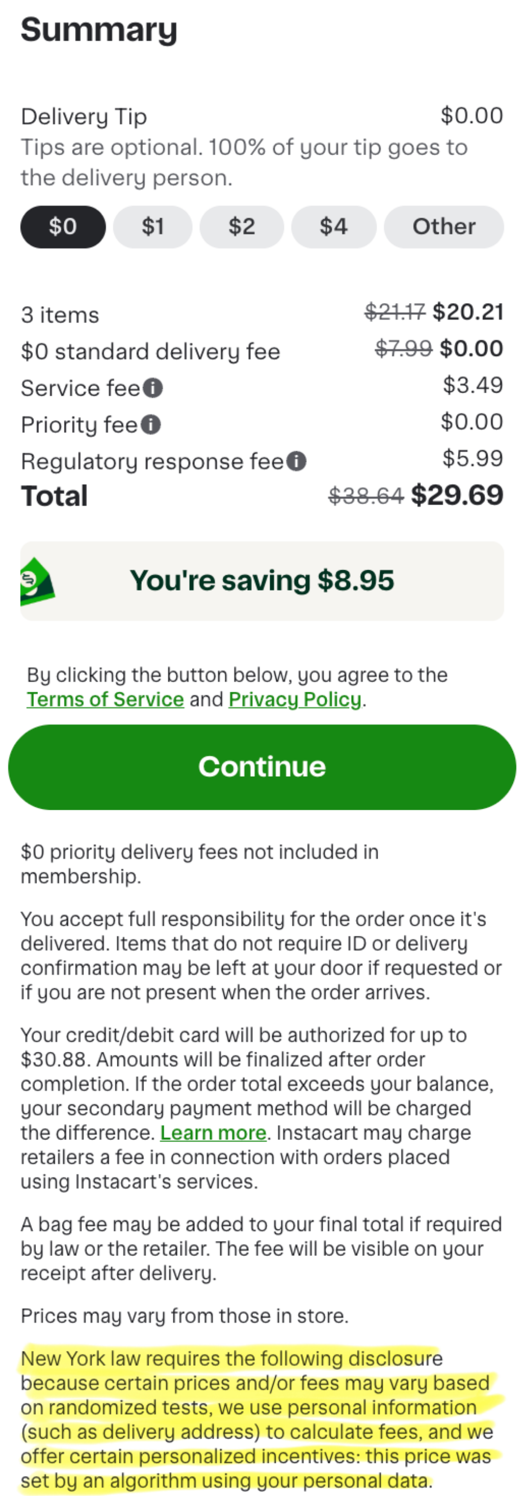
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)

/s/ Patrick K. Lin
Deputy Director
NYU Technology Law & Policy Clinic
Emily Dai
Tanika Deuskar
Sarah Wang

WASHINGTON SQUARE LEGAL
SERVICES, INC.
New York University School of Law
245 Sullivan Street, 5th Floor
New York, NY 10012
212-998-6430 (tel)

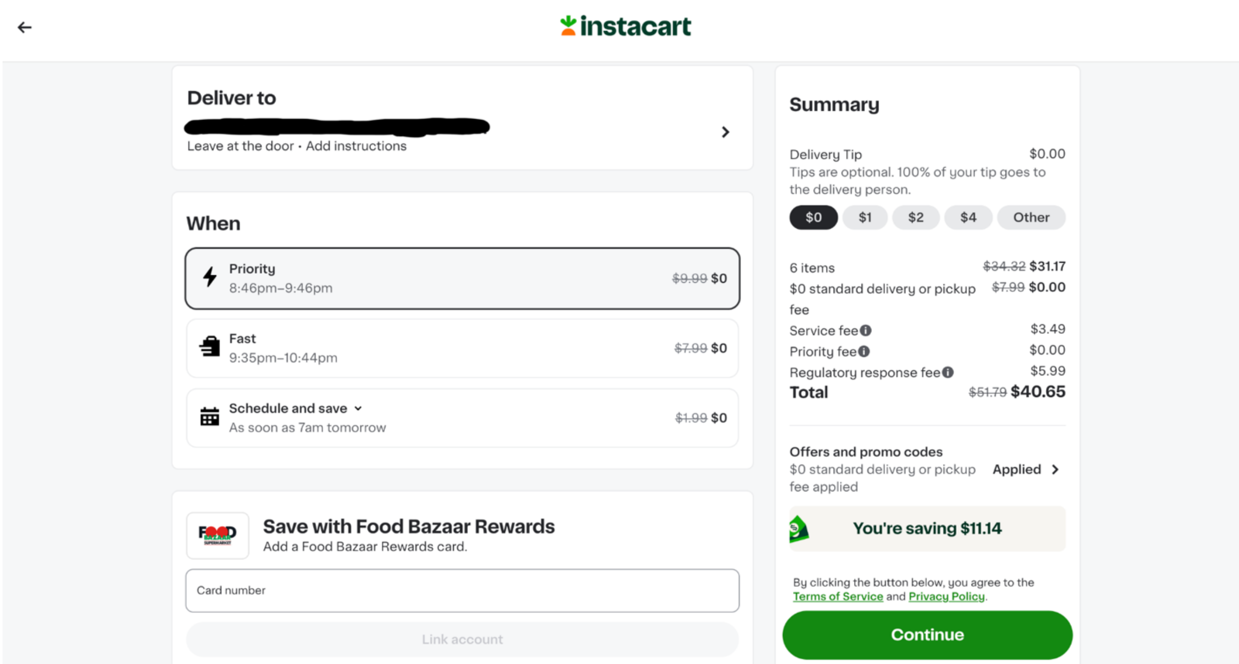
APPENDIX A

A. "In response, companies like Instacart have provided the following disclosure:" (p. 20)

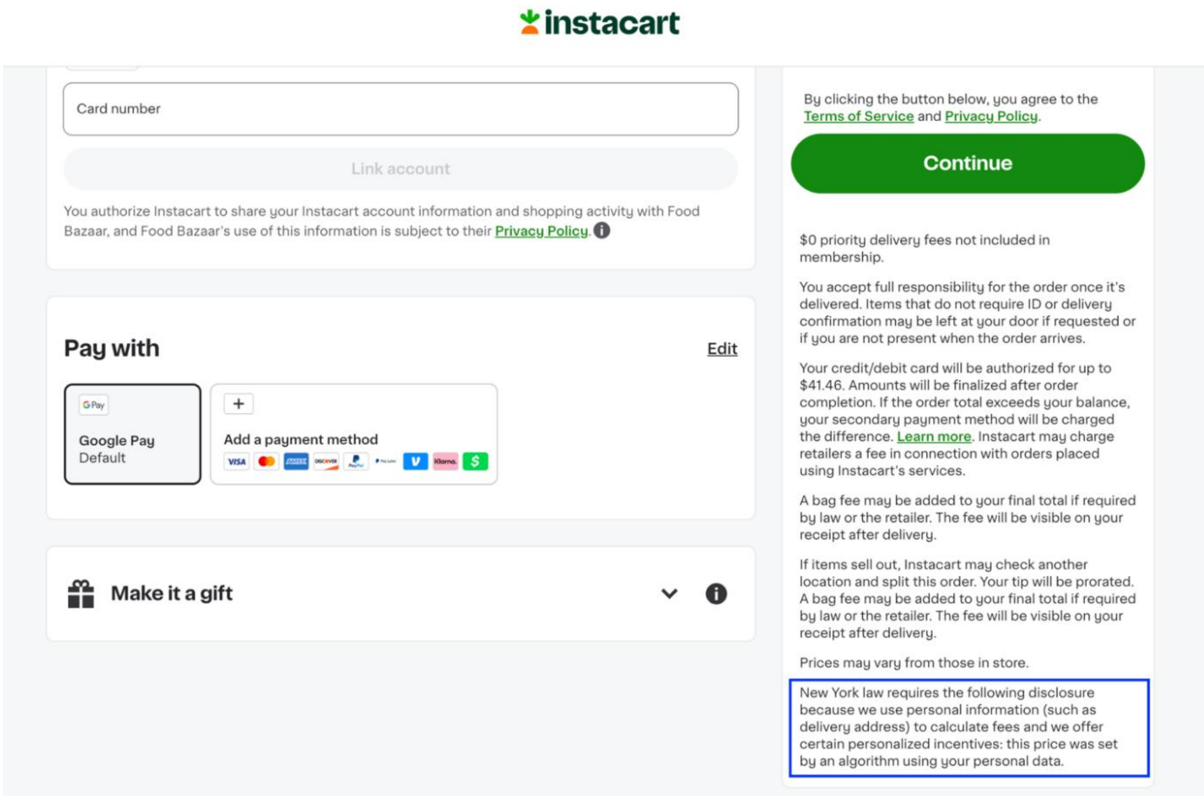


B. “When viewing websites on a computer, disclosures are typically placed below the button used to continue the transaction (e.g., Instacart, Aldi) [1] or are hidden behind an “information” icon (e.g., Target) [2]. Similarly, when on a mobile application, disclosures are placed at the bottom of the screen. Consumers have to intentionally scroll to the bottom of the screen, typically below the “checkout” button, to view the disclosure. [3] As a result, consumers can complete the transaction without ever encountering the disclosure.” (Footnote 67)

[1]

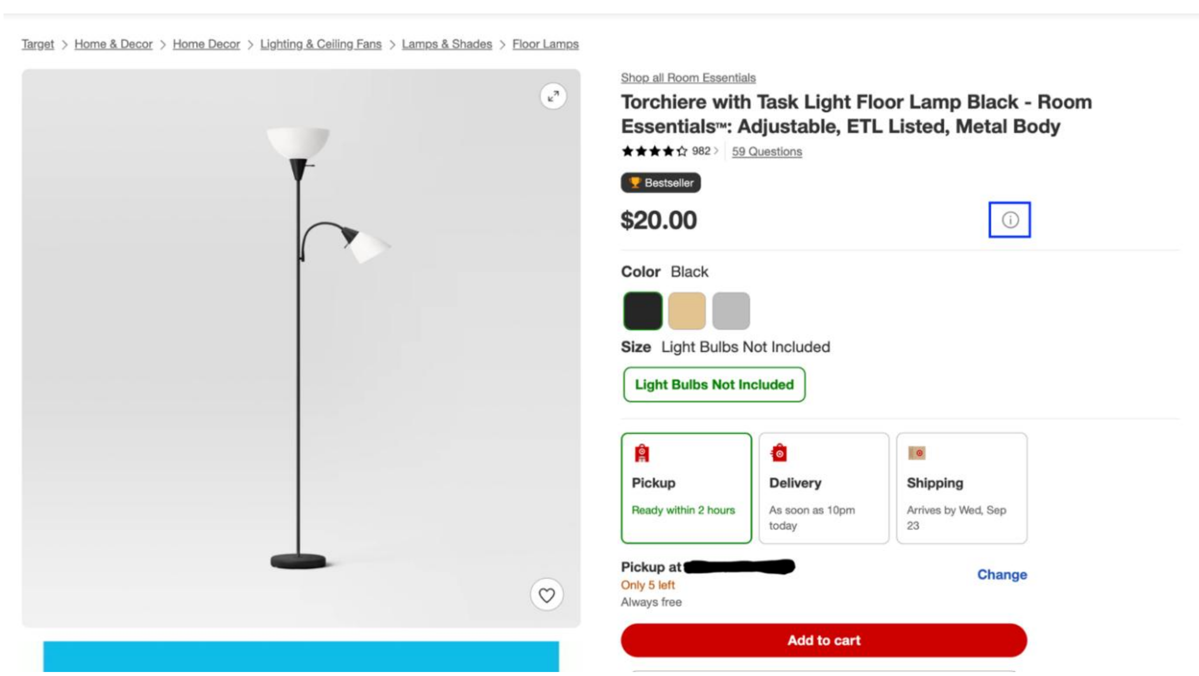


Instacart screen on a computer. Cannot see the disclosure without scrolling (see below).

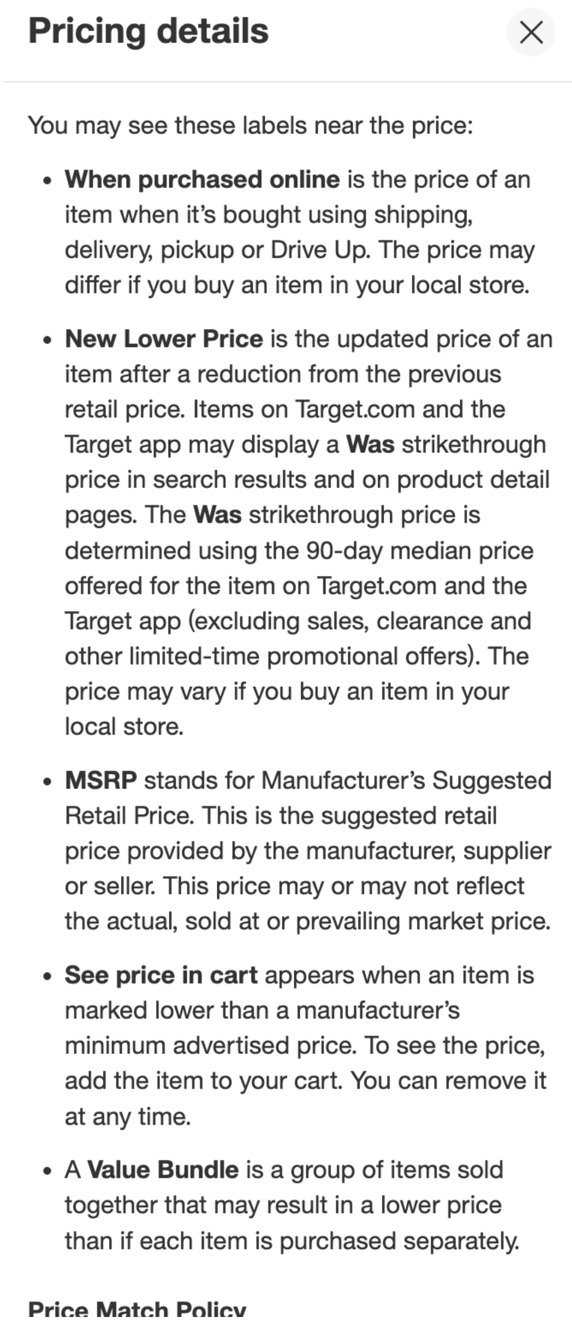


A user needs to scroll substantially to find the disclosure. The disclosure follows several other disclosures.

[2]



Clicking on the information icon (i) displays the following information.

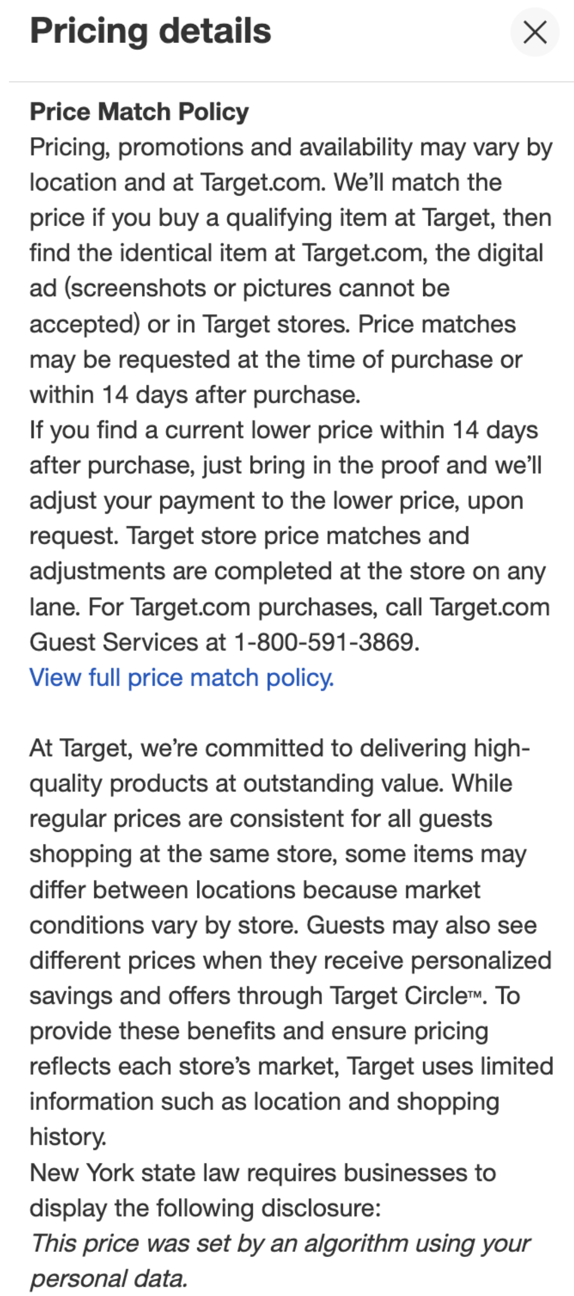


Pricing details

You may see these labels near the price:

- **When purchased online** is the price of an item when it's bought using shipping, delivery, pickup or Drive Up. The price may differ if you buy an item in your local store.
- **New Lower Price** is the updated price of an item after a reduction from the previous retail price. Items on Target.com and the Target app may display a **Was** strikethrough price in search results and on product detail pages. The **Was** strikethrough price is determined using the 90-day median price offered for the item on Target.com and the Target app (excluding sales, clearance and other limited-time promotional offers). The price may vary if you buy an item in your local store.
- **MSRP** stands for Manufacturer's Suggested Retail Price. This is the suggested retail price provided by the manufacturer, supplier or seller. This price may or may not reflect the actual, sold at or prevailing market price.
- **See price in cart** appears when an item is marked lower than a manufacturer's minimum advertised price. To see the price, add the item to your cart. You can remove it at any time.
- A **Value Bundle** is a group of items sold together that may result in a lower price than if each item is purchased separately.

Price Match Policy



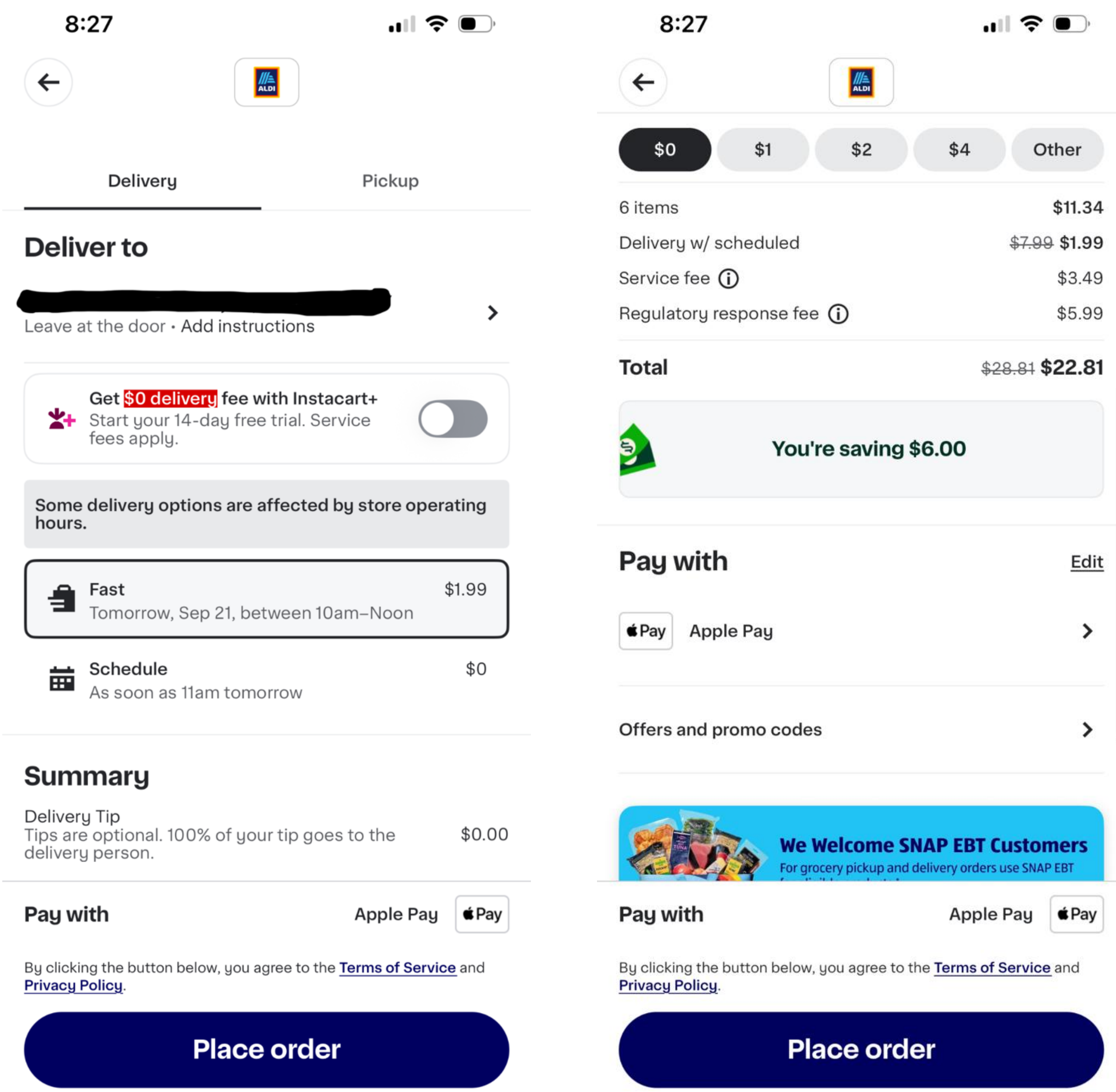
Pricing details

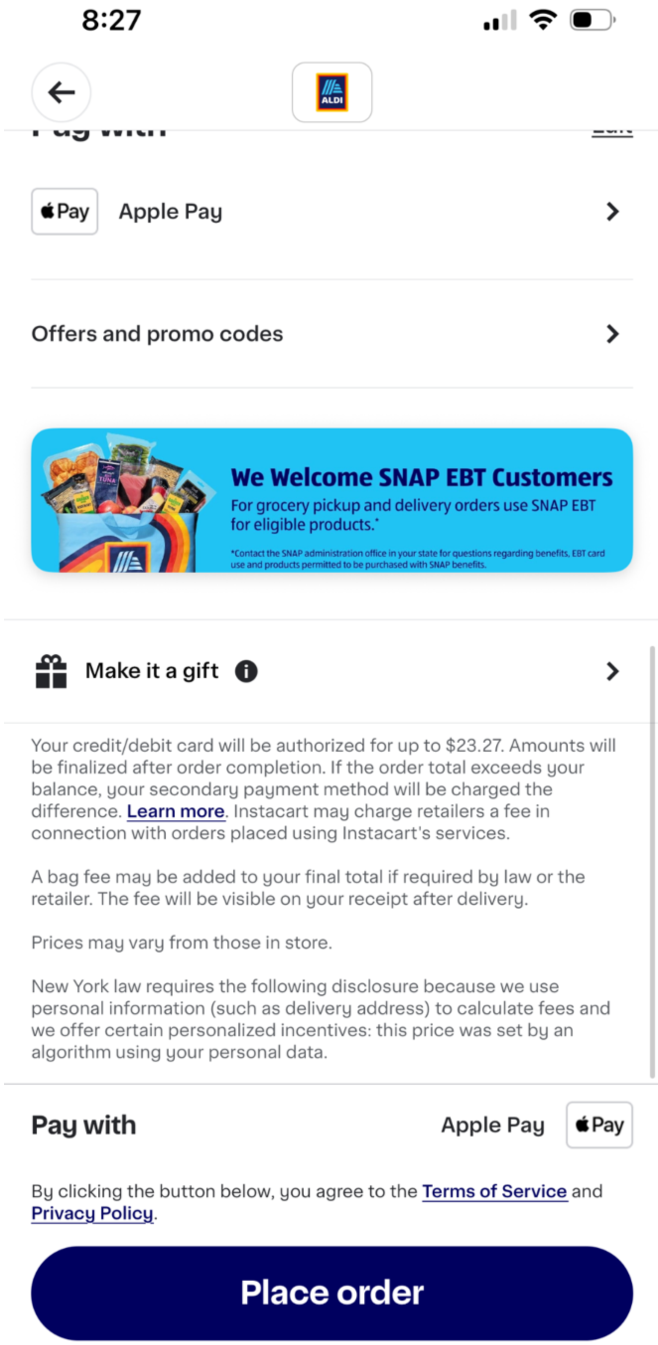
Price Match Policy
Pricing, promotions and availability may vary by location and at Target.com. We'll match the price if you buy a qualifying item at Target, then find the identical item at Target.com, the digital ad (screenshots or pictures cannot be accepted) or in Target stores. Price matches may be requested at the time of purchase or within 14 days after purchase.
If you find a current lower price within 14 days after purchase, just bring in the proof and we'll adjust your payment to the lower price, upon request. Target store price matches and adjustments are completed at the store on any lane. For Target.com purchases, call Target.com Guest Services at 1-800-591-3869.
View full price match policy.

At Target, we're committed to delivering high-quality products at outstanding value. While regular prices are consistent for all guests shopping at the same store, some items may differ between locations because market conditions vary by store. Guests may also see different prices when they receive personalized savings and offers through Target Circle™. To provide these benefits and ensure pricing reflects each store's market, Target uses limited information such as location and shopping history.
New York state law requires businesses to display the following disclosure:
This price was set by an algorithm using your personal data.

Users have to scroll down to the bottom of a lot of text to find the disclosure.

[3]

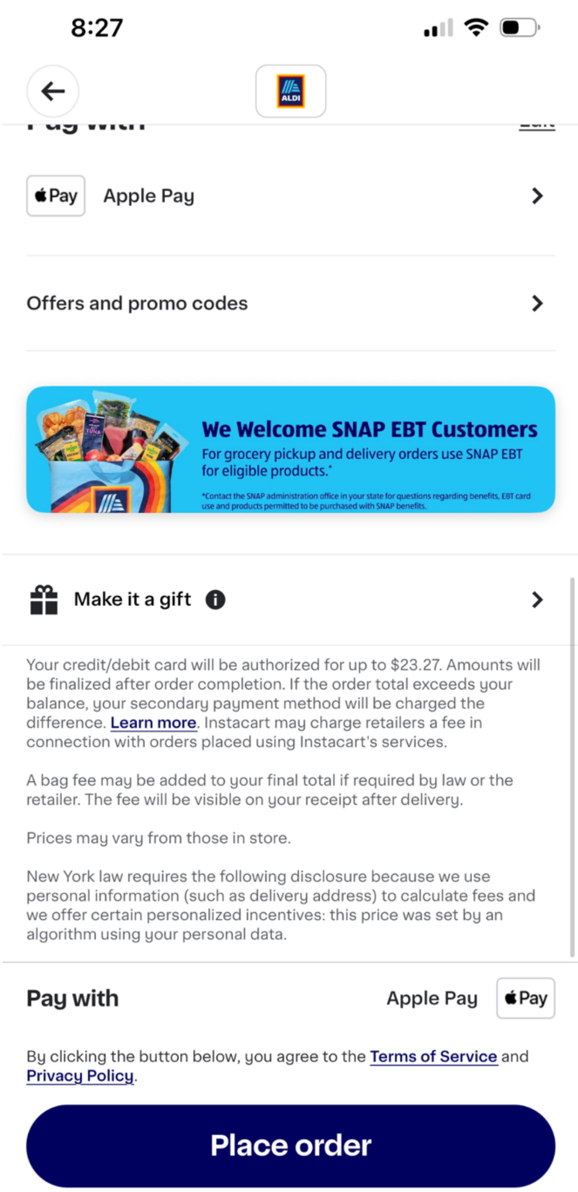

8:27
Delivery
Pickup
Deliver to
[redacted]
Leave at the door • Add instructions
Get $0 delivery fee with Instacart+
Start your 14-day free trial. Service fees apply.
Some delivery options are affected by store operating hours.
Fast
$1.99
Tomorrow, Sep 21, between 10am–Noon
Schedule
$0
As soon as 11am tomorrow
Summary
Delivery Tip
Tips are optional. 100% of your tip goes to the delivery person.
$0.00
Pay with
Apple Pay
Pay
By clicking the button below, you agree to the Terms of Service and Privacy Policy.
Place order
8:27
$0
$1
$2
$4
Other
6 items
$11.34
Delivery w/ scheduled
$7.99 $1.99
Service fee
$3.49
Regulatory response fee
$5.99
Total
$28.81 $22.81
You're saving $6.00
Pay with
Edit
Pay
Apple Pay
Offers and promo codes
We Welcome SNAP EBT Customers
For grocery pickup and delivery orders use SNAP EBT
Pay with
Apple Pay
Pay
By clicking the button below, you agree to the Terms of Service and Privacy Policy.
Place order



Users can easily place an order without seeing the disclosure.

C. “Based on disclosures in compliance with the New York Algorithmic Pricing Disclosure Act, Aldi [1], Target [2], Food Bazaar [3], and Instacart [4] all set prices using personal data.” (p. 14)

[1] Aldi



[2] Target

Pricing details

Price Match Policy

Pricing, promotions and availability may vary by location and at Target.com. We'll match the price if you buy a qualifying item at Target, then find the identical item at Target.com, the digital ad (screenshots or pictures cannot be accepted) or in Target stores. Price matches may be requested at the time of purchase or within 14 days after purchase.

If you find a current lower price within 14 days after purchase, just bring in the proof and we'll adjust your payment to the lower price, upon request. Target store price matches and adjustments are completed at the store on any lane. For Target.com purchases, call Target.com Guest Services at 1-800-591-3869.

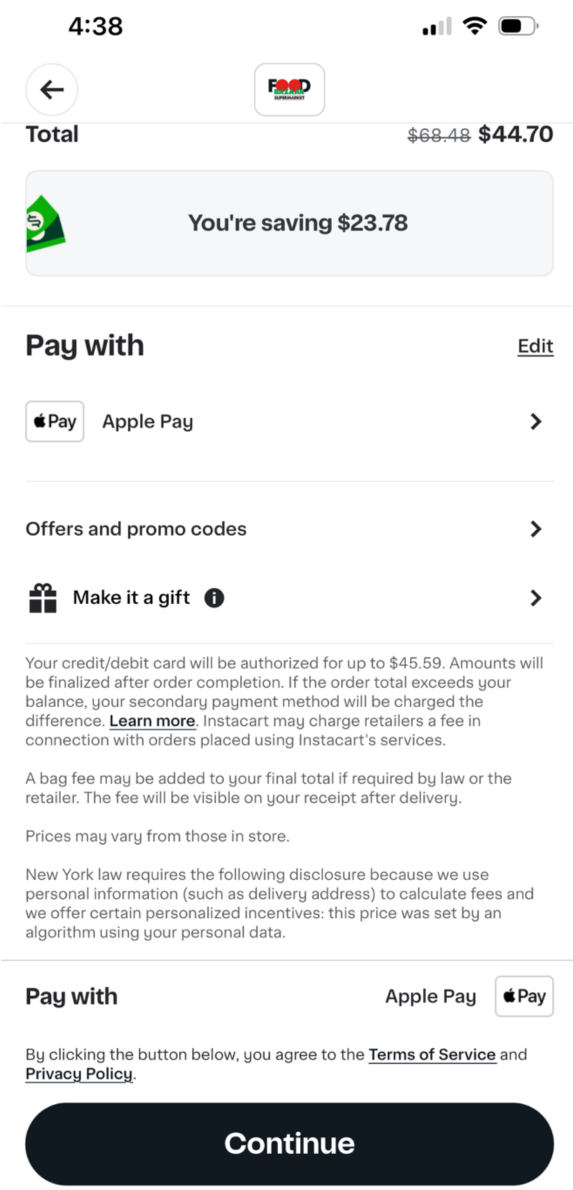
View full price match policy.

At Target, we're committed to delivering high-quality products at outstanding value. While regular prices are consistent for all guests shopping at the same store, some items may differ between locations because market conditions vary by store. Guests may also see different prices when they receive personalized savings and offers through Target Circle™. To provide these benefits and ensure pricing reflects each store's market, Target uses limited information such as location and shopping history.

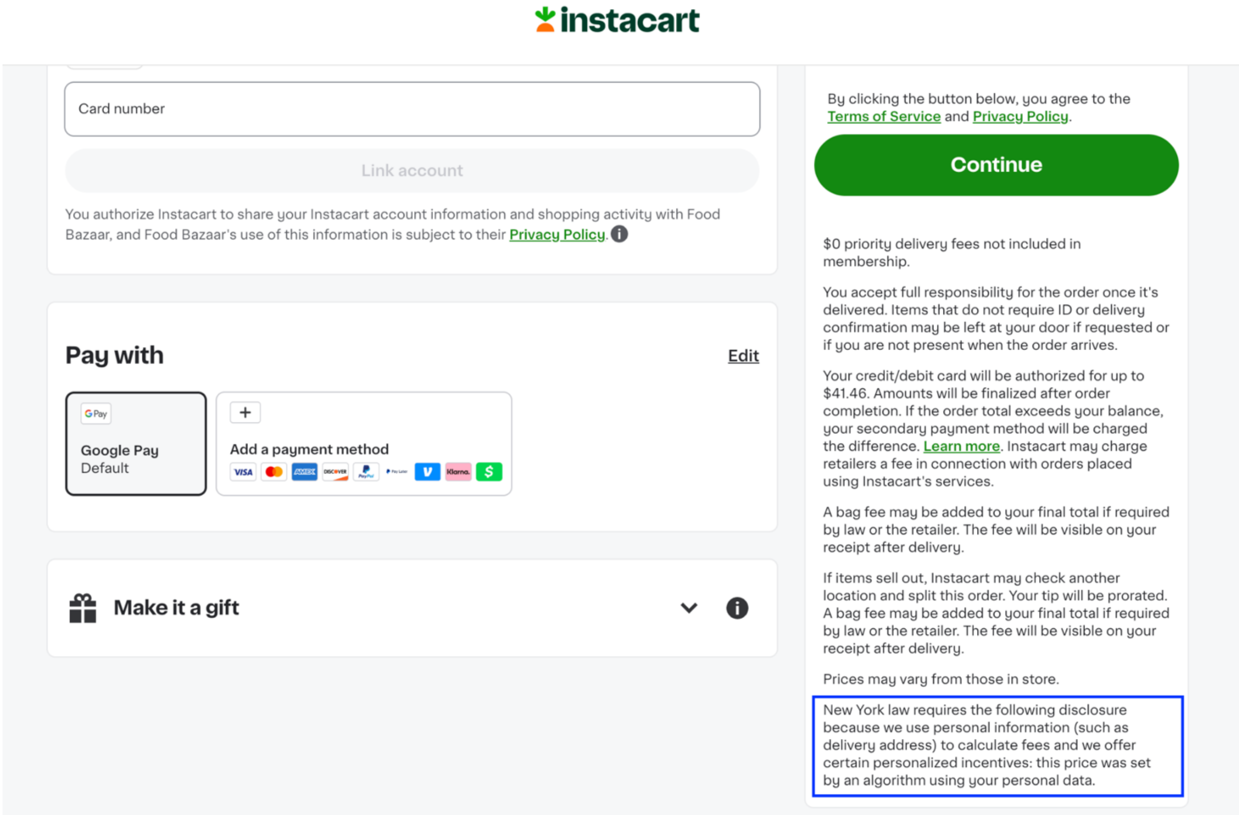
New York state law requires businesses to display the following disclosure:

This price was set by an algorithm using your personal data.

[3] Food Bazaar

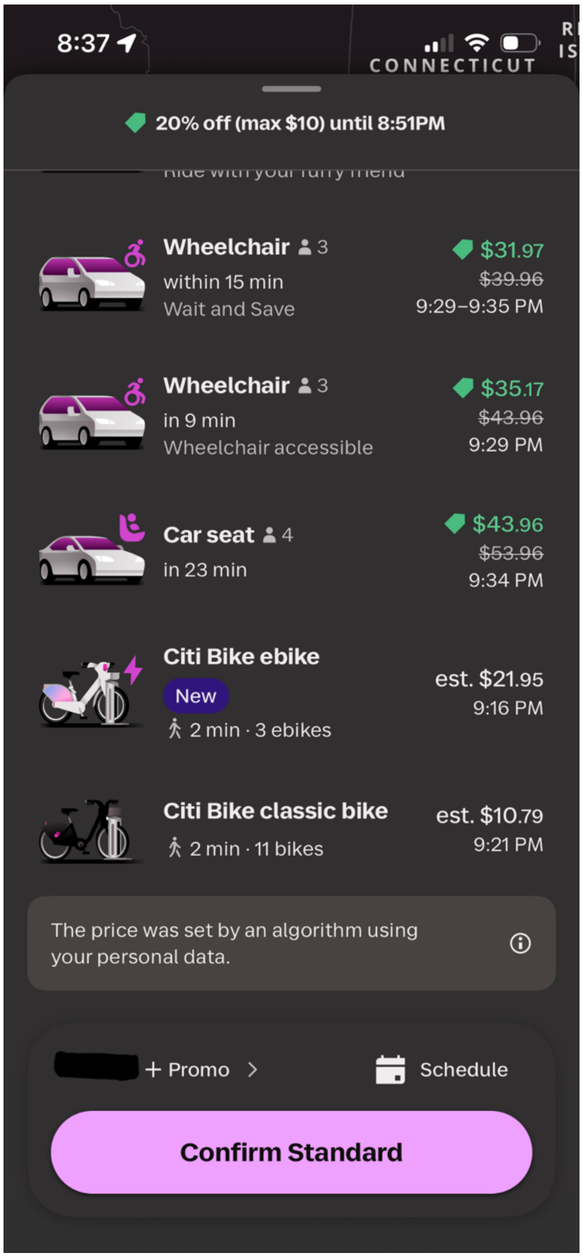


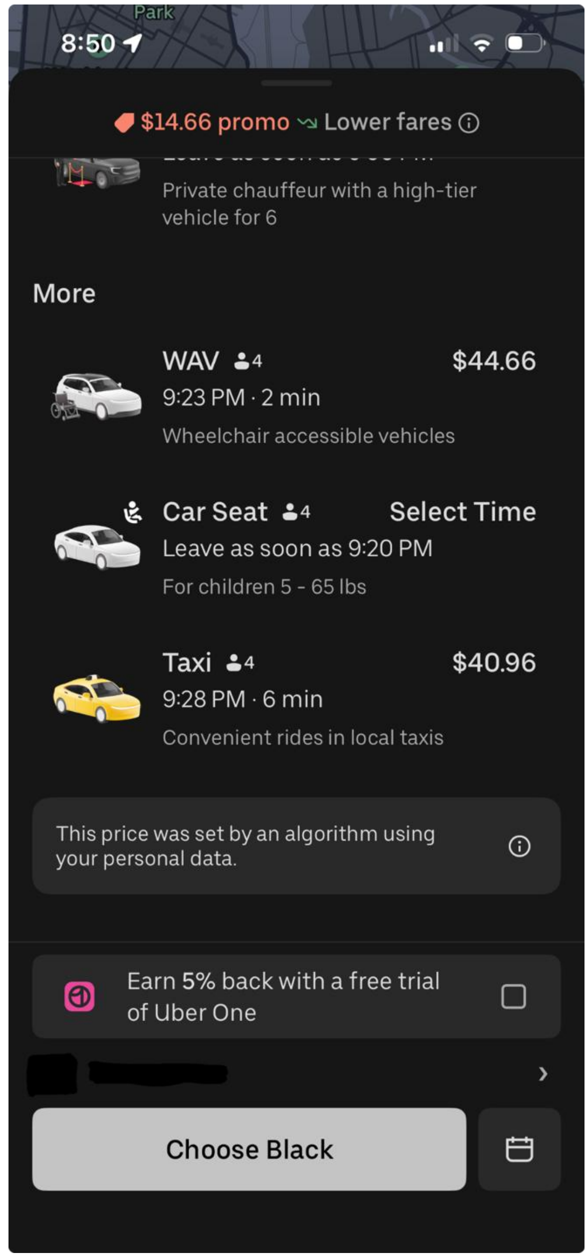
[4] Instacart


instacart
Card number
Link account
You authorize Instacart to share your Instacart account information and shopping activity with Food Bazaar, and Food Bazaar's use of this information is subject to their Privacy Policy.
Pay with
Edit
Google Pay
Default
Add a payment method
Make it a gift
By clicking the button below, you agree to the Terms of Service and Privacy Policy.
Continue
$0 priority delivery fees not included in membership.
You accept full responsibility for the order once it's delivered. Items that do not require ID or delivery confirmation may be left at your door if requested or if you are not present when the order arrives.
Your credit/debit card will be authorized for up to $41.46. Amounts will be finalized after order completion. If the order total exceeds your balance, your secondary payment method will be charged the difference. Learn more. Instacart may charge retailers a fee in connection with orders placed using Instacart's services.
A bag fee may be added to your final total if required by law or the retailer. The fee will be visible on your receipt after delivery.
If items sell out, Instacart may check another location and split this order. Your tip will be prorated. A bag fee may be added to your final total if required by law or the retailer. The fee will be visible on your receipt after delivery.
Prices may vary from those in store.
New York law requires the following disclosure because we use personal information (such as delivery address) to calculate fees and we offer certain personalized incentives: this price was set by an algorithm using your personal data.

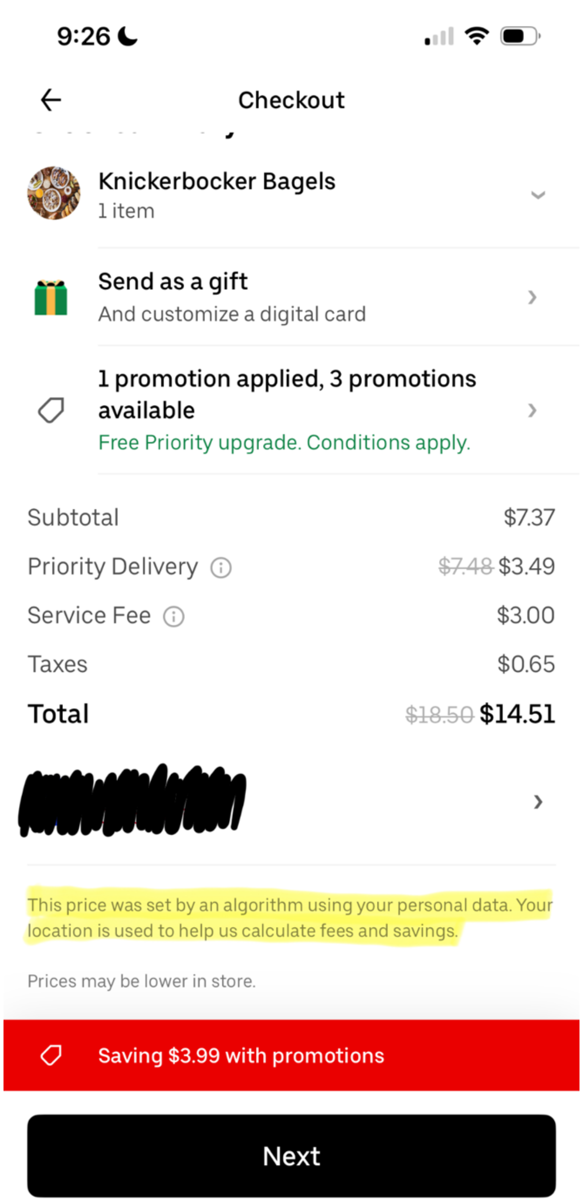
D. The same applies in other sectors: both Lyft [1] and Uber [2] seem to engage in surveillance pricing, as do UberEats [3], Grubhub [4], Postmates [5], Doordash [6] and Seamless [7]. (p. 14–15)

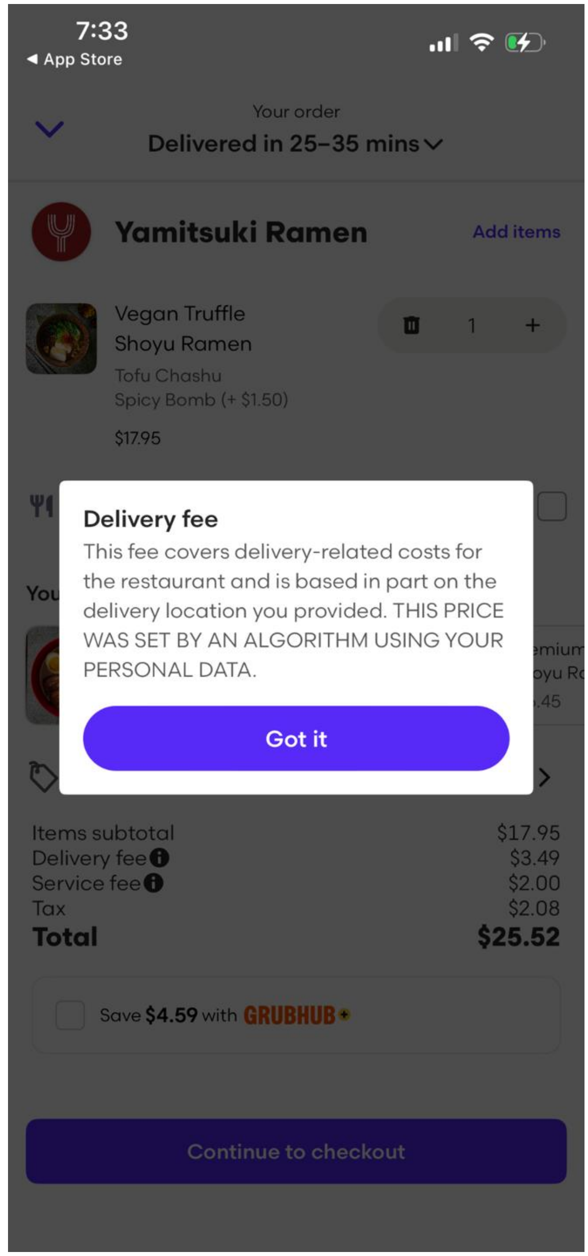
[1] Lyft, [2] Uber



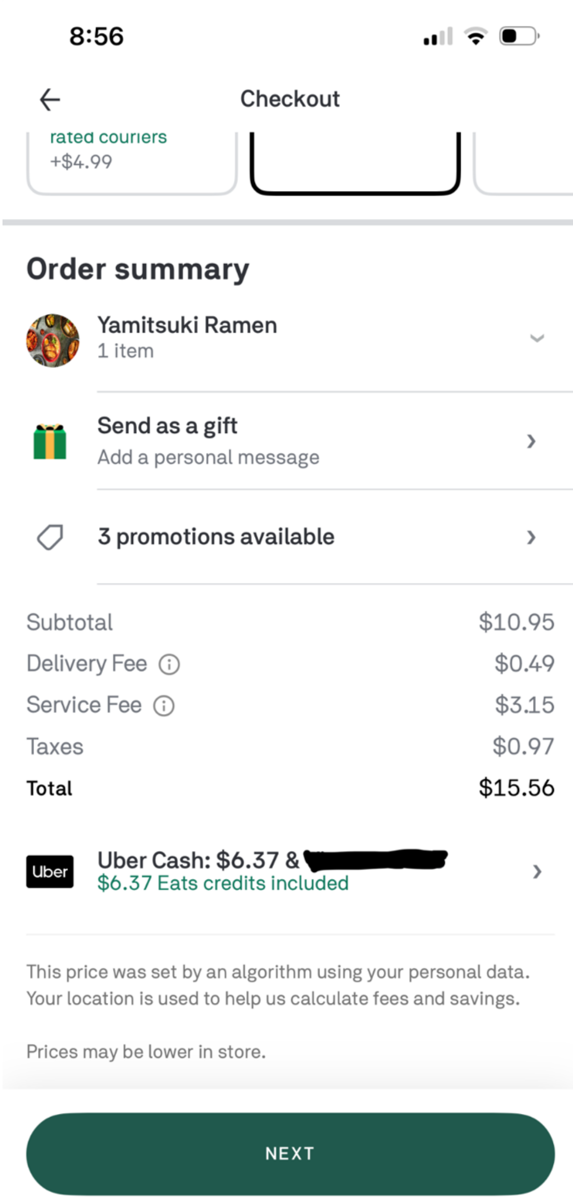


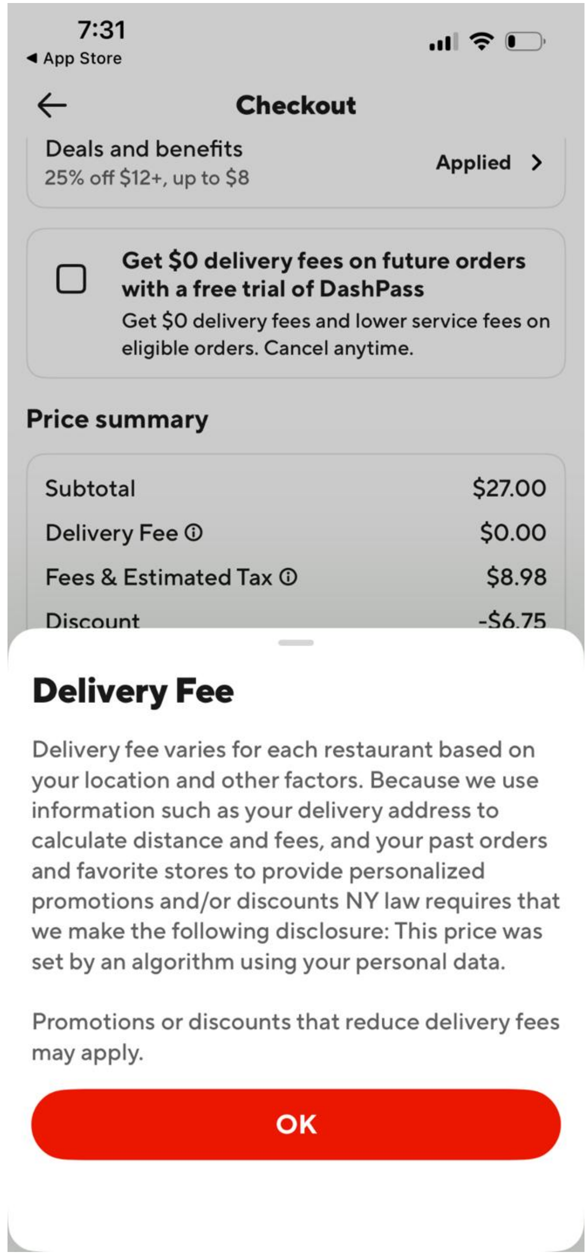
[3] Uber Eats, GrubHub



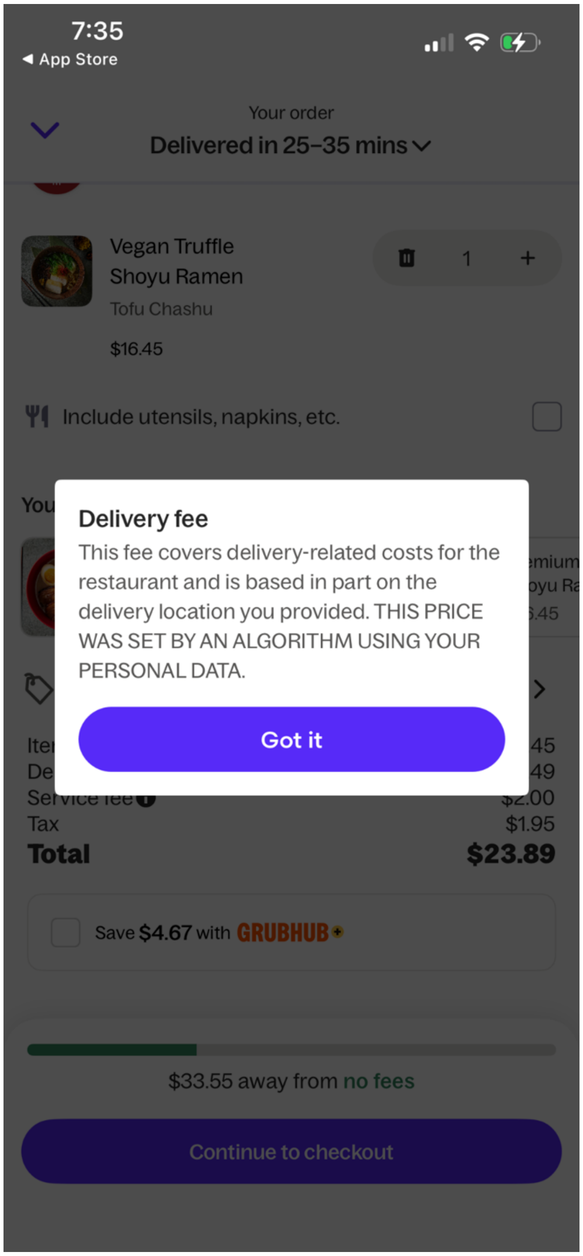


[5] Postmates, [6] DoorDash





[7] Seamless



7:35
App Store
Your order
Delivered in 25–35 mins
Vegan Truffle Shoyu Ramen
Tofu Chashu
$16.45
1
Include utensils, napkins, etc.
Delivery fee
This fee covers delivery-related costs for the restaurant and is based in part on the delivery location you provided. THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA.
Got it
Tax
$1.95
Total
$23.89
Save $4.67 with GRUBHUB+
$33.55 away from no fees
Continue to checkout