

May 14, 2026

New Jersey General Assembly
Assembly Commerce and Economic Development Committee

Dear Chair Spearman, Vice Chair Haider, and Members of the Committee:

EPIC writes in support of A 4085, the Fair Price Protection Act, to protect New Jerseyans from the unfair and harmful practice of surveillance pricing. New Jersey has the opportunity to further its leadership in consumer protection and tech policy by advancing this important legislation. At a time when everyone is concerned about fairness and affordability, the impact of harmful practices like surveillance pricing cannot be ignored.

The Electronic Privacy Information Center (EPIC) is an independent non-profit research organization based in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.¹ EPIC has advocated for strong AI, privacy, and consumer protection laws at both the state and federal levels for many years.²

Surveillance pricing regulation is urgently needed, and New Jersey should act now.

Legislation like the Fair Price Protection Act is critical to address the harms caused by companies using personal data to set individualized prices for consumers. Retailers have long sought to charge the highest amount consumers are willing to pay for a product or service to maximize their profits.³ Until recently, retailers were forced to set a single price for a market— all similarly situated customers saw the same price and decided whether they would or would not pay it. Today, the combination of advanced algorithms and troves of personal data on individual customers allow retailers to practice price discrimination, inferring the prices individual consumers are willing to pay and targeting their prices accordingly.⁴

¹ EPIC, *About EPIC*, <https://epic.org/about/>.

² See e.g., Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection & Comm. of the H. Comm. on Energy & Comm., 117th Cong. (2022) (testimony of Caitriona Fitzgerald, Deputy Director, EPIC), https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf; *EPIC Testifies in Support of Maryland Bill on High-Risk AI*, EPIC (Feb. 27, 2025), <https://epic.org/epic-testifies-in-support-of-maryland-bill-on-high-risk-ai/>.

³ Wells, Owens, Han & Smith, Groundwork Collaborative & Consumer Reports, *Same Cart, Different Price: Instacart's Price Experiments Cost Families at Checkout* 4–5 (2025), <http://groundworkcollaborative.org/wp-content/uploads/2025/12/Same-Cart-Different-Price.pdf> [hereinafter "Instacart Investigation"].

⁴ FTC, *FTC Surveillance Pricing 6(b) Study: Research Summaries, A Staff Perspective* 5 (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf [hereinafter "FTC Study"].

Surveillance pricing can involve disturbingly sensitive and varied personal information on an individual. Retailers can access enormous amounts of data both by collecting data firsthand from their customers and by purchasing data from data brokers.⁵ Data brokers gather data about consumers as they engage a wide range of activities in today’s economy.⁶ Data brokers then use this information to profile, categorize, and make inferences about individuals based on the personal data collected about them, including location, purchase history, economic status, mental and physical health conditions, or specific vulnerabilities.⁷ For example, consumers may be categorized as expectant mothers, older people struggling financially, people with symptoms of depression, people struggling with addiction, or people interested in weight loss, among countless other intimate categories.⁸

Surveillance pricing algorithms can make real-time price adjustments based on these detailed consumer profiles and customer responses in both brick-and-mortar stores and online.⁹ For example, a major investigation of Instacart found that the platform conducted surreptitious pricing experiments by varying grocery prices by tens of cents, making the changes difficult for consumers to detect but potentially resulting in an increased grocery cost of \$1,200 a year for the average customer.¹⁰ Using surveillance pricing tools, businesses can significantly increase their profits at the direct detriment of everyday consumers.

Surveillance pricing is an unfair practice that violates consumers’ reasonable expectations that the price of goods or services reflects their real value and the market as a whole—not exploitation of shoppers’ individual personal data. In a time when the cost of living is rising and more people are living paycheck-to-paycheck, surveillance pricing often targets the people who can least afford increased cost.¹¹

With key amendments, A 4085 could provide even stronger protections for New Jersey consumers.

This bill takes important steps to protect New Jerseyans from the harms of surveillance pricing. However, EPIC recommends three key amendments that would ensure this bill would

⁵ FTC Study at 8–9.

⁶ FTC Study at 8–9; Mayu Tobin-Miyaji, EPIC, *Assessing the Assessments: Maximizing the Effectiveness of Algorithmic & Privacy Risk Assessments* 6–7 (2025), <https://epic.org/assessing-the-assessments/>.

⁷ FTC Study at 2 n. 10, 4.

⁸ Jon Keegan & Joel Eastwood, *From “Heavy Purchasers” of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, The Markup (June 8, 2023), <https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you>.

⁹ FTC Study at 3–7; Instacart-owned Eversight, which sells pricing tools, admits that shoppers will see different prices. *Eversight by Instacart: AI-Powered Price Optimization*, Instacart Platform (last accessed Jan. 28, 2026), <https://www.instacart.com/company/retailer-platform/connected-stores/eversight>.

¹⁰ Instacart Investigation at 3.

¹¹ Seth Frotman & Tara Mikkilineni, *The Trump Administration Wants to Reboot Redlining*, Jolt Digest (July 7, 2025), <https://jolt.law.harvard.edu/digest/the-trump-administration-wants-to-reboot-redlining>.

properly address the harms while allowing businesses to continue to offer legitimate, fair, and transparent discounts to customers.

The bill should be expanded to cover third-party delivery services.

EPIC recommends expanding the bill’s scope to also include third-party delivery services, such as Instacart or DoorDash. These delivery services have been caught engaging in unfair surveillance pricing, and all other states that have passed legislation prohibiting surveillance pricing this year—Maryland, Connecticut, and Colorado—have included these third-party delivery services within the scope of their laws. We would recommend that New Jersey also prohibit these companies from engaging in surveillance pricing.

The terms “surveillance pricing” and “personalized algorithmic pricing” should be combined.

EPIC recommends that the bill only include a defined term for, and regulate, “surveillance pricing,” instead of including both “surveillance pricing” and “personalized algorithmic pricing.” As currently written, these definitions largely overlap, and the terms almost always appear together in the bill’s operative sections. To reduce redundancy and potential confusion, EPIC recommends retaining the definition of “surveillance pricing,” striking the definition of “personalized algorithmic pricing,” and striking references to personalized algorithmic pricing from the bill.

Exemptions for discounts and loyalty programs should be clarified further.

Discounts and loyalty rewards programs can be good for consumers, but they can also be cover for surveillance pricing depending on how they are operated. This legislation acknowledges this dynamic by exempting several kinds of widely used discount programs, including transparent and uniformly offered discounts, discounts for groups of people like teachers or veterans, and discounts offered as part of a loyalty program. However, EPIC is concerned that the definition of “bona fide discount” and the loyalty program exemption create a loophole that companies could easily exploit to continue engaging in unfair surveillance pricing practices.

Recent research and experience have shown that abusive loyalty programs can promise loyalty perks while, in reality, delivering loyalty penalties.¹² By collecting or purchasing reams of data about loyalty program participants, companies can determine who should get a coupon and who should not based on a consumer’s inferred price sensitivity and whether they would be willing to buy at a higher price.¹³ This practice is fundamentally unfair—some loyalty shoppers

¹² Samuel A.A. Levine & Stephanie T. Nyugen, *The Loyalty Trap: How Loyalty Programs Hook Us with Deals, Hack our Brains, and Hike Our Prices*, Vanderbilt Policy Center at 6, 14–21 (2025), <https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2025/10/17195957/The-Loyalty-Trap.pdf>.

¹³ FTC Study at 3.

should not be charged more than others in ways that they do not know or expect based on their personal data.

Individualized loyalty program vendors are not shy about this practice. For example, Eagle Eye is a popular vendor of individualized pricing technologies, and it boasts that it sends out more than a billion individualized discounts per week and includes in its list of current and former customers retail giants such as Petco, Rite-Aid, and major grocery stores.¹⁴ On its webpage advertising its personalized promotions product, it markets its technology as helping retailers avoid “customers [being] rewarded for behavior they would have delivered anyway” and “avoiding over-discounting customers who would have purchased anyway.”¹⁵ This is not a loyalty perk—it is a loyalty penalty that occurs when companies are able to send out secret, individualized discounts.

Individualized algorithmic discounting can also harm consumers by enabling price increases that are hard to detect. Businesses may claim that they only use individualized algorithmic pricing to provide “discounts” or to “decrease prices,” but discounts are meaningless without an established and stable baseline price for a good. Otherwise, businesses may simply artificially raise prices across the board, then offer individualized “discounts” to arrive at the same surveillance pricing outcome they would have otherwise.

The definition of “bona fide discount” and the language in Section 3(b)(3) should be tightened to ensure these kinds of unfair practices do not fall into this exemption. Companies should not be able to hide higher prices behind the façade of a loyalty program.

* * *

EPIC urges the Committee to advance this bill because the threat to privacy and affordability posed by surveillance pricing is an urgent problem. Thank you for the opportunity to testify today, and EPIC is happy to be a resource to the Committee on these issues.

Sincerely,

/s/ Tom McBrien
Tom McBrien
EPIC Counsel

/s/ Kara Williams
Kara Williams
EPIC Counsel

/s/ Mayu Tobin-Miyaji
Mayu Tobin-Miyaji
EPIC Law Fellow

¹⁴ Eagle Eye, <https://eagleeye.com/>.

¹⁵ Eagle Eye, *Personalized Promotions*, <https://web.archive.org/web/20260421150620/https://eagleeye.com/personalized-promotions>.