epic.org

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

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

April 21, 2026

Colorado General Assembly
Senate Committee on Business, Labor & Technology
200 E Colfax Avenue
Denver, CO 80203

Dear Chair Danielson and Members of the Committee,

EPIC writes in support of HB26-1210, Prohibiting Individualized Price and Wage Setting Using Surveillance Data, to further protect Coloradans from these harmful practices. Colorado has the opportunity to further its leadership in protecting the rights, privacy, and financial security of Colorado residents and workers with this proposal. At a time when policymakers are concerned about affordability for their constituents, the impact of practices like surveillance pricing and wage setting 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 Colorado should act now.

Legislation like HB26-1210 is critical to address the harms caused by companies using AI systems 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 allows

[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"].

retailers to practice price discrimination, inferring the prices individual consumers are willing to pay and targeting those prices accordingly.[4]

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]

Fueled by these detailed consumer profiles, surveillance pricing algorithms can make real-time price adjustments based on these 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 expectation that the price of goods or services reflects value and the market as a whole—not exploitation of their individual personal data. In a time of rising cost of living and more people living paycheck-to-paycheck, surveillance pricing often targets the people who can least afford increased cost.[11]

---

[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"].
[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, F*rom "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.

The bill takes a nuanced, reasonable, pro-consumer approach to discounts and loyalty programs.

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. HB26-1210 does an admirable job of exempting the kinds of discounts and loyalty rewards that consumers actually expect and benefit from while not exempting the kinds of discounts and loyalty rewards programs that defy consumers' expectations and are easier for companies to use to exploit consumers' personal data.

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 customers, 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] It is unfair that some loyalty shoppers are 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. Eagle Eye is a vendor of individualized pricing technologies that boasts 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. As an illustrative example, if a business set the base price of a six-pack as $5.99 for some consumers and $7.99 for others based on their personal data, many would deem this unfair. But if, instead, a business changed the base price of a six-pack to $7.99 for everyone, knowing that it could give more price-sensitive customers a coupon for $2 off without giving more price insensitive customers a coupon at all,

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

that would recreate the surveillance pricing outcome that consumers hate but shrouded in "discount" language that obscures what is really happening.

HB26-1210 properly disallows this kind of abusive discounting while permitting businesses to continue to provide the kinds of discounts that consumers like and actually benefit from, even ones based on personal data. It preserves discounts based on volume of goods bought (something like a coffee shop "get your tenth coffee free" punch card), discounts for loyalty customers, discounts offered as a retention strategy for unhappy customers, equal discounts for groups such as veterans and seniors, and more. This structure permits companies leeway in how to attract and retain consumers without risking re-creating the surveillance pricing infrastructure that the bill otherwise prohibits.

Automated wage setting based on surveillance data requires urgent legislative action.

Surveillance wage setting transforms wage determination from a fair calculation based on work performed to an exploitative system that gleans how little a worker is willing to accept in wages based on troves of their individual personal data.[16] Surveillance wage setting is a tactic for corporations employing workers to minimize costs, not through innovation but through exploitation of workers' personal data. Millions of U.S. workers are already subject to surveillance wages through gig work, such as driving for Uber, Lyft, or other food delivery companies.[17] This framework is rapidly expanding into other industries, such as nursing.[18]

Employers using algorithmic surveillance wage determinations results in unfair low wages, instability and precarity for workers, and lack of transparency. A study into the experience of nurses working for on-demand nursing companies found that those platforms incentivize nurses to bid lower wages against one another, create unstable and unpredictable schedules and sudden scheduling changes, take little accountability for worker safety, and ultimately threaten patient well-being.[19] Studies of on-demand drivers also show companies charging consumers more, paying workers less, and increasing profit through algorithmic price and wage setting.[20] A 2022 research study from Colorado Jobs With Justice with Colorado Independent Drivers United surveying hundreds of gig workers in the Denver area found drivers on average took home $5.49 an hour after expenses, significantly below Denver's 2022

[16] Veena Dubal & Wilneida Negrón, *How Artificial Intelligence Uncouples Hard Work from Fair Wages Through 'Surveillance Pay' Practices—and How to Fix it*, Washington Center for Equitable Growth (Aug. 21, 2025), https://equitablegrowth.org/how-artificial-intelligence-uncouples-hard-work-from-fair-wages-through-surveillance-pay-practices-and-how-to-fix-it/.
[17] AI Now Institute et al., *Prohibiting Surveillance Prices and Wages* 5–6 (2025), https://towardsjustice.org/wp-content/uploads/2025/02/Real-Surveillance-Prices-and-Wages-Report.pdf.
[18] Wells & Spilda, *Uber for Nursing: How an AI-Powered Gig Model is Threatening Health Care*, Roosevelt Inst. (Dec. 2024), https://rooseveltinstitute.org/wp-content/uploads/2024/12/RI_Uber-for-Nursing_Brief_202412.pdf.
[19] *Id*.
[20] Len Sherman, *Will Other Companies Follow Uber's Lead Into The Black Hole of Opaque Algorithmic Pricing?*, Medium (Sept. 16, 2025), https://len-sherman.medium.com/will-other-companies-follow-ubers-lead-into-the-black-hole-of-opaque-algorithmic-pricing-d79acd9cfe35.

minimum wage.[21] Some drivers report experiencing their work as a form of gambling and trickery, where the worker has little wage predictability based on the work they perform.[22]

HB26-1210 would be a strong step toward ensuring workers get paid fairly for their work. The bill would prohibit the use of personal data that does not relate to the performance of tasks that the worker was hired to perform. This ensures that employers don't take advantage of workers by offering lower pay based on data unrelated to work performance. The bill would also ensure increased transparency and accountability by requiring any company using an automated decision system to assist or replace human decision-making related to wages to develop and publish procedures to ensure accuracy of the data considered, for workers to request and receive information regarding what data is used and how it is considered for setting wages, and to challenge the accuracy of the data considered. These protections, coupled with the private right of action, would go far to ensure that Colorado workers are paid fairly.

Enforcement is critical.

Robust enforcement is critical to effective privacy protection. Strong state enforcement via Attorney General authority is a key part of any strong consumer protection law, and funds should be appropriated to ensure the Attorney General can meaningfully enforce the law.

However, while government enforcement is vital, a private right of action ensures that companies have strong financial incentives to comply with privacy laws. Evidence of this is seen in Illinois,[23] where a biometric privacy law passed in 2008 includes a private right of action. Lawsuits under that law have led to changes in harmful business practices, such as forcing facial recognition company Clearview AI to stop selling its face surveillance system to private companies.[24] In contrast, in states where Attorneys General have sole enforcement authority, there has been little enforcement of, and compliance with, privacy laws.[25]

Many privacy laws include a private right of action, allowing individuals to hold companies accountable for privacy violations.[26] Colorado residents have had the right to enforce their consumer rights in court under the Colorado Consumer Protection Act for decades. There is

---

[21] Kari Paul, *Colorado Gig Drivers Make an Average of Just $5.49 an Hour, Study Finds*, The Guardian (Nov. 9, 2022), https://www.theguardian.com/us-news/2022/nov/09/gig-drivers-colorado-wages-less-than-minimum-study.
[22] Veena Dubal, *On Algorithmic Wage Discrimination*, 123 Colum. L. Rev. 1929 (2023); Reuben Binns, Jake Stein, Siddhartha Datta, Max Van Kleek & Nigel Shadbolt, *Not Even Nice Work If You Can Get It; A Longitudinal Study of Uber's Algorithmic Pay and Pricing*, arXiv (June 18, 2025), https://arxiv.org/abs/2506.15278.
[23] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-hartzog.pdf.
[24] Ryan Mac & Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database*, N.Y. Times (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.
[25] *See generally* Consumer Reports, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws* (Apr. 2025), https://innovation.consumerreports.org/new-report-many-companies-may-be-ignoring-opt-out-requests-under-state-privacy-laws/.
[26] *See* Lauren Henry Scholz, *Private Rights of Action in Privacy Laws*, 63 Wm. & Mary L. Rev. 1639 (2022), https://scholarship.law.wm.edu/wmlr/vol63/iss5/5.

no reason privacy violations should be treated differently from other consumer rights violations. We encourage the Committee to keep this provision.

With amendments, HB26-1210 could provide even stronger protections for Colorado residents.

HB26-1210 takes important steps to protect Coloradans from the harms of surveillance pricing and automated wage setting. However, while the bill includes "locations frequented" in the definition of "Behaviors," adding precise geolocation data[27] under the definition of "Personal Characteristics" would avoid confusion and make clear that such data about an individual cannot be used to conduct surveillance pricing or individualized wage setting. This would still allow companies to use non-precise, or course, location data to set prices in different areas of the state, but including "precise geolocation data" in the definition of "behaviors" would have two advantages: one, it disincentivizes the collection of this particularly sensitive form of data in the first place, and two, it prevents companies from using our precise comings and goings, to unfairly determine prices.

We also recommend that the bill be adapted to explicitly ban use of device specifications, such as what model phone a consumer is using or how low their battery is, in setting prices.[28]

* * *

EPIC urges the Committee to support this bill because the threat to privacy and affordability caused by surveillance pricing and algorithmic wage setting 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
Counsel, EPIC

/s/ Calli Schroeder
Calli Schroeder
Senior Counsel, EPIC

/s/ Kara Williams
Kara Williams
Counsel, EPIC

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

[27] As defined under C.R.S. 6-1-1303(17.5).
[28] *Uber Accused of Charging People More If Their Phone Battery Is Low*, Vice (Apr. 11, 2023), https://www.vice.com/en/article/uber-surge-pricing-phone-battery/.