March 12, 2026

Colorado House Business Affairs & Labor Committee
200 E. 14th Street
Denver, CO 80203

Re: Opposition to House Bill 1210 — Prohibiting Individualized Price and Wage Setting Using Surveillance Data

Dear Chair Naquetta Ricks, Vice Chair Sean Camacho, and Members of the House Business Affairs & Labor Committee:

On behalf of the Travel Technology Association (Travel Tech) and our members, thank you for the opportunity to submit comments regarding House Bill 1210, which would prohibit the use of individualized data for automated wage and price setting decision systems.

Travel Tech represents the leading innovators in travel technology, including Online Travel Agencies (OTAs), metasearch engines, Global Distribution Systems, short-term rental platforms, and Travel Management Companies. Our members generally do not set the underlying prices of airline seats, hotel rooms, or rental cars. Rather, they operate digital platforms that display supplier-set inventory and, in some cases, offer consumer-facing discounts, loyalty-based pricing programs, and contextual promotions designed to deliver value to travelers.

While Travel Tech supports protecting consumers from predatory data practices, HB 1210 as currently drafted goes far beyond those harms. The bill would directly impair the dynamic pricing systems that power competitive travel markets, impose disproportionate litigation exposure, and ultimately harm the very consumers it aims to protect. We respectfully submit the following comments and recommendations.

I. The Bill's Definitions of "Surveillance Data" and "Automated Decision System" are Overbroad

HB 1210 defines "surveillance data" to include purchase history, browsing history, location data, financial circumstances, and inferred consumer behaviors. For Travel Tech members, this data underlies virtually every consumer interaction — not for exploitation, but to surface relevant offers, match travelers with available inventory, and ensure competitive pricing in real time. The bill does not distinguish between data used to prey on vulnerable consumers and data used to deliver a better, more competitive travel experience. As written, the definition would capture routine platform operations that have nothing in common with the predatory use cases — such as charging a diabetic more for insulin supplies or paying a desperate worker less — that the bill's legislative declaration identifies as its target.

The bill also defines "automated decision system" to include any technology that uses statistical modeling, data analytics, or artificial intelligence to assist or inform human decision-making.

This definition captures standard revenue management tools that have no relationship to the predatory conduct described in the bill's declaration. The breadth of this definition, combined with the private right of action and per-transaction penalty structure, would create significant legal uncertainty for Travel Tech members about whether widely used, consumer-beneficial pricing tools fall within the bill's prohibitions — chilling investment in the very technology that makes competitive travel pricing possible.

Proposed Fix: Narrow "surveillance data" and "automated decision system" to focus on personally identifiable data or sensitive characteristics or practices that could be used to exploit consumer vulnerability, and explicitly exclude data used solely for supply-and-demand-based pricing, loyalty programs, or other common, pro-consumer operations.

II. All Consumer-Beneficial Discounts Should Be Expressly Exempted

The bill attempts to preserve legitimate pricing practices by carving out "temporal differences, including dynamic pricing and price fluctuations based on supply and demand." Adjusting fares and rates in real time based on availability, demand, and market conditions is fundamental to how competitive travel markets function and how consumers access the most relevant and affordable options.

However, the carve-out applies only where differential pricing is not informed by surveillance data. In practice, modern revenue management systems rely on multiple inputs simultaneously, including supply and demand signals, historical purchasing patterns, and other consumer-related data. The bill draws no clear line between these inputs, leaving platforms exposed to enforcement risk for pricing practices that are routine, transparent, and widely used across competitive markets.

From a policy perspective, there is no clear distinction between a price change driven by market demand and one informed by data signals that help platforms present the most relevant options to consumers. A traveler searching for flights on short notice, for example, benefits from a platform that can surface available inventory and competitive prices based on real-time market conditions and prior search activity. Yet under HB 1210, these integrated systems could fall outside the bill's limited dynamic pricing carve-out simply because they rely on non-personal consumer-related data inputs.

The result is a regulatory structure that creates uncertainty around widely used and consumer-beneficial pricing practices. Faced with ambiguous compliance obligations and potential litigation exposure, companies may conclude that the safest course is to scale back data-informed pricing tools and discounting mechanisms for Colorado consumers.

Proposed Fix: Narrow the scope of the measure to the use of personally identifiable data and strengthen the dynamic pricing carve-out to explicitly protect revenue management systems, loyalty discounts, cross-sell offers, and other routine, consumer-beneficial promotions.

III. Enforcement Should Be Limited to the Attorney General

HB 1210 authorizes enforcement by the Attorney General, district attorneys, and private plaintiffs, and makes violations actionable under Colorado's consumer protection laws. While public enforcement plays an important role in protecting consumers, the bill's inclusion of a broad private right of action raises significant concerns.

Under HB 1210, each consumer and each transaction may constitute a separate violation. The bill authorizes civil penalties of up to $10,000 per violation in actions brought by the Attorney General or a district attorney and up to $3,000 per violation in private actions, in addition to treble damages where bad faith is alleged. For Travel Tech members that process millions of transactions annually in Colorado, this structure creates potentially massive liability exposure that is wholly disproportionate to the conduct the bill seeks to address.

These risks are compounded by the fact that HB 1210 establishes novel regulatory obligations using newly defined or broadly framed concepts related to data use and pricing practices. Key terms lack an established interpretive history under Colorado law, creating substantial uncertainty for businesses attempting to comply. Allowing private litigation under these untested definitions invites speculative lawsuits that could characterize routine pricing practices or widely used technology tools as violations.

Limiting enforcement to the Attorney General would still provide meaningful accountability while ensuring that the statute develops through consistent, expert enforcement by state authorities. Public enforcement would allow regulators to prioritize cases involving genuine consumer harm while avoiding fragmented interpretations driven by private litigation.

Travel Tech therefore recommends amending HB 1210 to eliminate the bill's private right of action and limit enforcement authority to the Attorney General.

IV. Conclusion

Travel Tech does not oppose the legislature's interest in protecting Colorado consumers from genuinely exploitative data practices. However, HB 1210 as currently drafted would prohibit pricing practices that are transparent, pro-competitive, and beneficial to consumers — while exposing travel platforms to litigation exposure that bears no relationship to the harms the bill identifies. We urge the Committee to narrow the definition of "surveillance data" to exclude data used for supply and demand-based pricing, strengthen the dynamic pricing carve-out to explicitly protect revenue management systems, and remove or substantially limit the private right of action.

We stand ready to work with you and the relevant committee to develop targeted amendments that address legitimate concerns without creating incentives that reduce discounts, raise prices, or impose unworkable obligations on platforms that do not engage in individualized consumer profiling.

Thank you for your consideration.

Sincerely,

Laura Chadwick
President & CEO
The Travel Technology Association
www.traveltech.org

CC: The Honorable Jennifer Bacon

AAUW of Colorado

March 2026

To: House Business Affairs & Labor Committee

Re: AAUW SUPPORT HB1210--Prohibit Surveillance Price & Wage Setting

Dear Committee Members,

The American Association of University Women (AAUW) is one of the oldest women's organizations in the country, empowering women since 1881. The mission of AAUW is to advance equity for women and girls through research, education and advocacy. More than 700 community leaders are members of AAUW branches around Colorado.

Over the years, progress has been made in achieving economic security for women. Yet, hurdles remain, and now new hurdles are being created via the use of online surveillance of buying habits and earnings histories. Women are especially vulnerable due to our role as the caregivers for our families. We often do the majority of shopping, thus we are creating online profiles that can be used against us. We start out at lower pay than our male counterparts and that sets the bar lower far into our future earnings and retirement income. Our buying habits and earnings records should not be fair game for retailers and employers to take advantage of.

HB1210 prohibits discrimination against a consumer or worker through the use of these unfair practices; yet does not prohibit otherwise fair practices in pricing and wages.

AAUW of Colorado strongly supports House Bill 1210 and requests your YES vote in committee and throughout the process of becoming a law.

Thank you for your consideration,

Hon. Su Ryden
AAUW of Colorado Advocacy Director

16699 E. Kentucky Ave. • Aurora, CO 80017
303.898.5797
suryden25@gmail.com

American Association of University Women--AAUW is a top-rated 501(c)3 charitable organization whose mission is to advance gender equity for women and girls through research, education, and advocacy.

March 11, 2026
Colorado House of Representatives
House Business Affairs & Labor

Re: HB26-1210 - Prohibit Surveillance Price & Wage Setting

Dear Honorable Committee members,

HB26-1210 addresses an everyday affordability problem for consumers: surveillance pricing. Surveillance pricing, also sometimes referred to as "personalized" pricing, is when a company uses personal data that they've gathered about a consumer—like data about their online search history, their location, or inferences about family structure, health conditions, or income—to set the price of a product or determine the discount offered to a consumer. Consumer Reports[1] is strongly supportive of prohibiting surveillance pricing.

If enacted, this bill would make Colorado a leader on affordability. It prohibits surveillance pricing, while protecting transparently offered, non-discriminatory discounts. It builds on Colorado's data privacy and consumer protection statutes, while addressing a gap in the current law. Right now, nothing prohibits businesses from collecting or buying data about individual Coloradans, and then using that data against them to profile them and charge them a higher price than their neighbor. This bill would address that problem; Consumer Reports encourages an 'aye' vote.

What is surveillance pricing?

Not long ago, before the rise of online shopping and mass data collection, consumers could shop anonymously, confident that the price tag they saw on the shelf wasn't influenced by the store's knowledge of their family, shopping habits, online browsing, ability to pay, or any particular situation that could increase their urgency to purchase. That is no longer the case.

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

Companies can gather data on consumers' purchase histories, speed of click through, history of clicks, search history, 'likes' on social media, geolocation, IP address, device type, and more, to create a detailed portrait of a consumer. They can use artificial intelligence to make detailed inferences about consumers based on this data. These detailed profiles, combined with technology that enables companies to display different prices to different consumers online—or send discounts on an individualized basis—means that companies have all the tools they need to implement surveillance pricing. Retailers can understand when a consumer might be desperate enough to tolerate a higher price or when a loyal customer will keep coming back even in the absence of discounts.

A recent investigation from Consumer Reports, More Perfect Union and Groundwork Collaborative, revealed that Instacart, enabled by the artificial intelligence pricing software Eversight, was running large-scale, hidden price experiments on unsuspecting customers.[2] The team of journalists and researchers analyzed live shopping data from more than 400 Instacart shoppers across four U.S. cities. The findings show many U.S. shoppers who order grocery pickup and delivery through Instacart were unknowingly enrolled in AI-enabled experiments that can charge up to 23% more for the same item ordered from the same store at the same time.

Nearly three-quarters of grocery items tested on Instacart showed different prices to different shoppers. Some items carried up to five different price points simultaneously. For example, people shopping at a Safeway in Washington, D.C., saw a dozen Lucerne eggs listed at five different prices — $3.99, $4.28, $4.59, $4.69, and $4.79. The average price variations observed in the study could cost a household of four about $1,200 per year. Instacart's algorithmic pricing experiments were found to be occurring through the platform at several of the nation's biggest grocery retailers, including Albertsons, Costco, Kroger, Safeway, Sprouts Farmers Market, and Target.

Other enterprising journalists have conducted investigations and discovered examples of apparent surveillance pricing:

- An investigative journalist writing for SFGate looked at the prices offered for a hotel room in Manhattan for a specific date, and varied his operating system, browser, cookies, and location (his computer's IP address).[3] He found that when he changed his IP address from a Bay Area location to locations in Phoenix and Kansas City, the prices dropped by more than $200 per night in one instance, and more than $511 in another instance.

---

[2] Derek Kravitz, "Instacart's AI-Enabled Pricing Experiments May Be Inflating Your Grocery Bill, CR and Groundwork Collaborative Investigation Finds" *Consumer Reports,* Dec. 9, 2025, https://www.consumerreports.org/money/questionable-business-practices/instacart-ai-pricing-experiment-inflating-grocery-bills-a1142182490/

[3] Keith A. Spencer, "Hotel booking sites show higher prices to travelers from Bay Area," *SFGate,* Feb. 3, 2025. https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php

- ProPublica found that test-prep company Princeton Review was offering different prices for its tutoring services depending on a customer's zipcode.[4] The result, they found, was that Asian customers were nearly twice as likely to receive a higher price.
- The Wall Street Journal reported that Orbitz, the travel aggregation company, determined that Mac users spent more per night on hotels than Windows users, and began steering Mac users towards pricier hotels.[5]
- A Minnesota local news site discovered that Target changed the prices displayed on its app for certain products based on whether the customer—and their device—was physically inside a Target store. When the reporters looked at the Target app while inside a store, they found that a Graco car seat was $72 more expensive than when they had been sitting on the far side of the Target parking lot, and a Dyson vacuum was $148 more expensive.[6]

Surveillance pricing can hurt consumers by offering different prices based on a protected status, such as race or gender. It can also hurt consumers by pushing them to pay the most they are individually willing to pay, or by taking advantage of them in moments of desperation, when their willingness to pay increases. One hypothetical example offered by former chair of the Federal Trade Commission, Lina Kahn, is airlines charging an individual more for a plane ticket if the airline infers—based on the individual's search history—that there was a death in the family and the consumer needs to attend a funeral.[7]

There's another downside for consumers beyond potentially paying higher prices. Personalized pricing, especially personalized discounts that are offered through membership programs or are contingent on the use of certain mobile apps, can make the experience of finding a product's price and comparing across vendors much more time intensive and frustrating. This difficulty will have broader effects in the market, comparison shopping is an engine of market competition; retailers only feel the need to compete to offer the best price if consumers can comparison shop with ease, identify the best price, and make a decision based on that knowledge. As comparison shopping becomes more cumbersome for consumers, the competitive pressure decreases.

---

[4] Julia Angwin, Surya Mattu and Jeff Larson, "The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review," *ProPublica,* Sept. 1, 2015 https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review

[5] *Dana Mattioli,* "On Orbitz, Mac Users Steered to Pricier Hotels," *Wall Street Journal,* Aug. 23, 2012 https://www.wsj.com/articles/SB10001424052702304458604577488822667325882

[6] Chris Hrapsky, "The Target app price switch: What you need to know" *Kare 11,* Jan. 27, 2019 https://www.kare11.com/article/money/consumer/the-target-app-price-switch-what-you-need-to-know/89-9ef4106a-895d-4522-8a00-c15cff0a0514

[7] Jaures Yip, "FTC chair Lina Khan warns that airlines might one day use AI to find out you're attending a funeral and charge more," *Business Insider,* September 23, 2024 https://www.businessinsider.com/ftc-chair-lina-khan-warns-ai-pricing-discrimination-risks-2024-9

What HB26-1210 does

HB26-1210 prohibits the use of data related to a person's characteristics, behavior, or biometrics to automatically and secretly inform the price or wage they are offered. This includes, for example, data about a consumer's race or weight, their parenthood status, their genetic information, the geometry of their face, their political affiliations, their location, and their web-browsing history. HB26-1210 also prohibits the secret and automated use of surveillance data to target groups of individuals with prices. This is important because the fine-grained data that companies possess about consumers enables them to place individuals into highly specific groups, such as "mothers of toddlers without higher education earning less than $75k" or "sports enthusiast male over 35 earning more than $150k." In a Consumer Reports investigation of Kroger's loyalty program data practices, consumers requested the data the grocer had collected about them. One consumer received a 62-page long profile, which included inferences about the size of his family, his education level, an estimate of his income, and other disparate information other companies might use to segment their shoppers for price targeting, including how likely he is to go on a cruise, have a pet, or travel internationally.[8]

HB26-1210 also has several reasonable exemptions from the prohibition on surveillance pricing. If a company can demonstrate that it offers different prices to different people based on differences in the cost of providing a good or service to different consumers, that practice is not surveillance pricing, and is not prohibited. There are also tailored exemptions for insurers relying on risk-relevant data, and for refusals to offer credit based on data covered by the Fair Credit Reporting Act. There are also important protections for discounts.

Protecting transparent discounts

Straightforward discounts and sales that everyone is eligible for and that do not rely on personal data are not impacted by this bill. The bill also protects transparently offered, non-discriminatory discounts—a crucial provision as discounting practices become more opaque and less trustworthy. More specifically, the bill protects three large categories of transparently offered discounts:

- Discounts that any consumer could potentially receive, so long as the eligibility criteria are publicly disclosed. This is a broad category that includes many common kinds of discounts, such as BOGO, discounts for signing up for a mailing list, discounts for related products (eg. 20% meals after you buy theme park tickets)—just about any kind of discount that is based on the consumer taking an action or making a purchase.
- Discounts that are offered to members of a broadly defined group, such as teachers, students, veterans, and seniors, so long as the eligibility criteria, terms, and discounts are

[8] Derek Kravitz, "Inside Kroger's Secret Shopper Profiles: Why You May Be Paying More Than Your Neighbors", Consumer Reports, May 21, 2025

clearly disclosed, and any consumer who can demonstrate they are part of the group can obtain the discount.
- Discounts that are offered through a loyalty or reward program, so long as prices are not individualized between consumers in the program, and current discounts, promotions, or benefits are publicly disclosed, and if the program offers a system for accruing or exchanging points, credits, any other non-monetary system, the program doesn't effectively personalize prices through that system.

Why require some transparency around discounts? Discounts are increasingly complex and opaque. Retailers can end-run around a ban on personalized pricing by increasing list prices and then offering "personalized discounts" based on individual's personal data and inferences about their willingness to pay. In the Staples example mentioned above, the office supplier seemingly inferred that consumers with easier access to competitor stores would have a lower willingness to pay. Consumers are also invasively profiled in the name of "personalized discounts." For example, pricing analysts at Target created an algorithm to predict the likelihood that a specific consumer is pregnant–based on their shopping habits–and then allocate discounts on the basis of that prediction.[9] An online casino was recently penalized by a UK regulator for advertising free spins and bonuses to someone who searched online "How to unsubscribe from all gambling," a possible indicator of gambling addiction.[10]

Suggested changes

While CR strongly supports a policy of prohibiting surveillance pricing, there is one tweak we suggest in order to ensure workability. Subdivision 4, relating to publication of procedures, need not apply to pricing. Since the bill already prohibits pricing based on personal data, the remaining data considered by automated decision systems would be non-personal data, such as various input costs. Giving consumers access to that information goes beyond the scope of what is necessary to address the harms of surveillance pricing. It is also unclear what pricing data consumers would be in a position to correct, given that this bill prohibits the use of their personal data to set prices.

[9] Charles Duhigg, "How companies learn your secrets," *The New York Times Magazine,* Feb. 16, 2012
[10] Rob Davies, "Online casino advert banned for targeting problem gamblers" The Guardian, Oct. 9, 2019*,*
https://www.theguardian.com/society/2019/oct/09/casumo-ad-banned-for-targeting-people-trying-to-stop-gambling

Overall, we are strongly supportive of prohibiting surveillance pricing. We appreciate the committee's consideration, and applaud Rep. Bacon, Rep. Mabrey, Sen. Weissman, and Sen. Jodeh for their leadership on this pocketbook issue.

Sincerely,
Grace Gedye
Senior Policy Analyst
Consumer Reports

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

March 11, 2026

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

Dear Chair Ricks 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 profit.[3] Until recently, retailers were forced to set a single price for a market—all 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 retailers to practice price

[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"].

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 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.

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.[12] 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.[13] This framework is rapidly expanding into other industries, such as nursing.[14]

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 scheduling changes, take little accountability for worker safety, and ultimately threaten patient well-being.[15] Studies of on-demand drivers also show companies charging consumers more, paying workers less, and increasing profit through algorithmic price and wage setting.[16] 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 minimum wage.[17] 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.[18]

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

[12] 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/.
[13] 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.
[14] 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.
[15] *Id*.
[16] 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.
[17] 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.
[18] 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.

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,[19] 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.[20] In contrast, in states where Attorneys General have sole enforcement authority, there has been little enforcement of, and compliance with, privacy laws.[21]

Many privacy laws include a private right of action, allowing individuals to hold companies accountable for privacy violations.[22] Colorado residents have had the right to enforce their consumer rights in court under the Colorado Consumer Protection Act for decades. There is 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[23] 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

[19] 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.
[20] 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.
[21] *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/.
[22] *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.
[23] As defined under C.R.S. 6-1-1303(17.5).

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.[24]

* * *

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/ Calli Schroeder
Calli Schroeder
Senior Counsel, EPIC

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

[24] *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/.