25-2818

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

NATIONAL RETAIL FEDERATION,

Plaintiff-Appellant,

v.

LETITIA JAMES, in her official capacity as Attorney General of New York,

Defendant-Appellee.

On Appeal from the United States District Court for the Southern District of New York

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLEE

Megan Iorio
Tom McBrien
Mayu Tobin-Miyaji
Hayden Davis
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

February 17, 2026

Attorneys for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amicus curiae* the Electronic Privacy Information Center states that it has a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF THE *AMICUS CURIAE*[1]

The Electronic Privacy Information Center ("EPIC") is a public interest organization in Washington, D.C., focused on emerging privacy, technology, and civil liberties issues. EPIC often participates as *amicus curiae* in cases concerning privacy rights and the First Amendment implications of data protection regulations, seeking to help courts to understand the relevant technological and policy considerations in cases to vindicate users' free speech and privacy rights. *See* EPIC, *The First Amendment* (2026).[2]

---

[1] No party's counsel authored any part of this brief. No one, apart from EPIC and its counsel, contributed money intended to fund the brief's preparation or submission. All parties consented to EPIC's filing this brief.

[2] https://epic.org/issues/platform-accountability-governance/the-first-amendment-and-platform-regulation/.

SUMMARY OF THE ARGUMENT

The National Retail Federation ("NRF") seeks to transform a business preference for consumer ignorance into a First Amendment right to commercial opacity. That turns the First Amendment on its head. Commercial speech jurisprudence, especially through the line established by *Zauderer v. Office of Disciplinary Counsel*, 471 U.S. 626 (1985), values consumers' right to information about commercial transactions, and defers to the state's decision to require businesses to provide truthful information to consumers. The state's power to mandate commercial disclosures is especially important in the digital age, where large corporations collect and process individuals' data in opaque ways with dramatic impacts on consumers' lives.

As part of the ongoing effort to arm individuals with information relevant to their commercial dealings, the State of New York enacted a consumer protection law, the Algorithmic Pricing Disclosure Act ("the Act"), to require transparency when businesses use personalized algorithmic pricing. *See* G.B.L. § 349-a.

The Act satisfies the prerequisites for *Zauderer*'s deferential form of scrutiny. It requires a straightforward and factual disclosure to

consumers when a company uses personalized algorithmic pricing. This is a personal data use disclosure requirement, which has been a common feature in data protection laws for decades. Just like calorie counts on a menu, the Act's disclosure is a canonical example of one to which *Zauderer* applies.

The Act satisfies *Zauderer* because the state's interest in passing this law is strong and the law is sufficiently tailored. The disclosure informs consumers of a commercial practice affecting everyday purchases about which they otherwise have no notice. Armed with this knowledge, consumers may choose to shop around. The disclosures also benefit consumers by helping them understand the practice's impact on the economy and society more broadly. The law properly exempts situations in which there is little harm to consumers from not being explicitly told whether a business is engaged in personalized algorithmic pricing, such as situations in which that is already assumed to be common practice. For these reasons, the Court should affirm the district court's order granting the defendant's motion to dismiss.

ARGUMENT

I. THE FIRST AMENDMENT INTEREST IN INFORMING CONSUMERS IS CRUCIALLY IMPORTANT IN THE DIGITAL AGE.

The values undergirding *Zauderer* are more important now than ever. Companies' use of computer technology to facilitate commercial transactions has powerful material effects on consumers' everyday lives, and these effects can be difficult for consumers to track and understand unless companies disclose their practices. In particular, companies' increasing use of opaque algorithms that operate on personal data impacts consumers in many ways. Companies use such algorithmic systems to determine the ads consumers see, the products they are recommended, and now the prices they pay. Companies also use algorithmic systems to gatekeep consumers' access to necessities such as employment, public benefits, housing, and health care. *See* T.M. Brown, *The Technology That Actually Runs Our World*, The Atlantic (Dec. 16, 2024).[3] The First Amendment's protection for the free flow of truthful information to consumers is vital to address information

[3] https://www.theatlantic.com/culture/archive/2024/12/cultural-algorithms/680987/.

asymmetries and power imbalances between consumers and the companies with which they transact.

Companies' increasing reliance on consumers' personal data means that Americans face significant privacy challenges in the modern economy. Many people do not know how their personal data is used and regret their inability to control it. In a 2023 survey conducted by Pew Research Center, 67 percent of Americans reported they "understand little to nothing about what companies are doing with their personal data," up from 59 percent in 2019. Colleen McClain *et al.*, *How Americans View Data Privacy*, Pew Res. Ctr. (Oct. 18, 2023).[4] A large majority strongly supports new laws to protect their privacy, *see id.*, but so far Congress and state legislatures have largely failed to act.

Consumers have good reason to be concerned about their lack of data privacy. In recent years, companies and state entities have repeatedly misused or insufficiently protected personal data in ways that have harmed consumers. Consumer smartphone apps have shared intimate consumer information with data brokers who sell it widely,

---

[4] https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

such as users' visits to medical facilities, houses of worship, and LGBTQ-related businesses. *See* Gabriel Hongsdusit, *Federal Trade Commission Sanctions Location Data Broker X-Mode*, The Markup (Jan. 11, 2024).[5] Data brokers have in turn been hacked by malicious foreign actors, spreading intimate details even further. *See* Justin Sherman, *These Pregnancy Apps May Be Sources for a Location Data Broker*, EPIC.org (Jan. 30, 2025).[6] Many companies have misled users about privacy practices, perhaps most famously Facebook when it enabled Cambridge Analytica to produce and sell psychological profiles of users to political campaigns and foreign governments. Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. Times (Apr. 4, 2018).[7] Research has shown that social media sites can use individuals' data to enable third parties to racially discriminate against users in housing and employment ads. *See* Jinyan Zang, *Solving the Problem of Racially Discriminatory*

---

[5] https://themarkup.org/privacy/2024/01/11/federal-trade-commission-sanctions-location-data-broker-x-mode.
[6] https://epic.org/these-pregnancy-apps-may-be-sources-for-a-location-data-broker/.
[7] https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Advertising on Facebook, Brookings Institute (Oct. 19, 2021).[8] In a world largely run on data, a consumer's lack of knowledge and control over how their personal data is used is a threat to their privacy and their safety.

To fix this kind of information and power disparity, the First Amendment allows states to require companies to disclose accurate, factual commercial information to consumers. *Zauderer*, 471 U.S. at 651. The free flow of factual commercial information to consumers is crucial for self-governance and consumer choice. *See Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 765 (1976). Data use disclosures help consumers understand the real terms of commercial transactions—both the data they are exchanging for services as well as how companies are using their data to decide what products and services to offer them and on what terms.

---

[8] https://www.brookings.edu/articles/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/.

II. THE ACT SATISFIES *ZAUDERER'S* "PURELY FACTUAL AND UNCONTROVERSIAL" PREREQUISITES.

Personalized algorithmic pricing is an increasingly widespread practice in which businesses use algorithms to set individualized prices based on the consumer's personal information. The goal is to maximize revenues. *See* Mark Abraham *et al.*, *The $70 Billion Prize in Personalized Offers*, Boston Consulting Group (Sept. 14, 2021).[9] Businesses use consumers' personal data to calculate their personal willingness to pay, which they can then use to set prices to the maximum that an individual is willing to pay or to induce purchases that a consumer would otherwise not have made. Without notice, there is little way for consumers to know that a company is using personalized algorithmic pricing. The Act's disclosure requirement remedies this situation through a straightforward and factual statement about whether the price a would-be customer sees was set using personalized algorithmic pricing.

---

[9] https://www.bcg.com/publications/2021/personalized-offers-have-a-potential-70-billion-dollar-growth-opportunity.

The Act's disclosure requirement is entitled to *Zauderer*'s deferential standard of scrutiny because it straightforwardly and accurately notifies consumers that a company uses personalized algorithmic pricing to set the price the consumer sees. This is a paradigmatic example of "'purely factual and uncontroversial information' about the goods or services the speaker may offer." *Volokh v. James*, 148 F.4th 71, 85–86 (2d Cir. 2025) (quoting *Zauderer*, 471 U.S. at 651).

A. Companies use algorithms to set prices based on consumers' personal data without consumers' knowledge.

Personalized algorithmic pricing involves using computer programs to set individualized prices for consumers based on insights about their identities and behaviors. Companies use this practice to increase revenue in a variety of ways, such as by setting a price to the highest that each individual customer is willing to pay or by inducing a consumer to purchase products they otherwise would not have. Federal Trade Commission, *FTC Surveillance Pricing 6(b) Study: Research Summaries — A Staff Perspective* 3–5 (Jan. 2025) [hereinafter "FTC

Study"].[10] The tactic is working. Businesses that have implemented personalized algorithmic pricing have seen significant increases in revenue. *See* Abraham *et al.*, *supra*.

The variety and amount of personal data companies use in their personalized algorithmic pricing algorithms is staggering. This data can include the consumer's location, internet browsing history, demographics such as age and gender, and inferences about income and urgency of need, among other variables. *See* FTC Study at 3; AI Now Institute *et al.*, *Prohibiting Surveillance Prices and Wages* 8 (2025).[11]

Companies are not limited to setting prices based on the information they personally collect from consumers. They can—and often do—access rich and voluminous data about consumers by purchasing personal information from data brokers. Jon Keegan, *Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data*

---

[10] https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf.

[11] http://www.economicliberties.us/wp-content/uploads/2025/02/Real-Surveillance-Prices-and-Wages-Report.pdf.

About You, The Markup (Feb. 16, 2023)[12]; FTC Study at 8–9. Data from data brokers is especially valuable because they aggregate disparate data sources into detailed profiles and extract powerful insights. FTC Study at 8–9; EPIC, Comments on CFPB Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information, 88 Fed. Reg. 16,951, 2–5 (July 14, 2023).[13] Data brokers group consumers into categories that reflect intimate characteristics such as expectant mothers, depressed people, people interested in weight loss, or people who are elderly and struggling financially. 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).[14] Armed with this data, algorithms can predict, among other things, how much an individual desires a product or service, how likely an

---

[12] https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you.
[13] https://epic.org/wp-content/uploads/2023/07/EPIC-CFPB-data-brokers-RFI-comments-071423.pdf.
[14] https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

individual is to search for competing products or services, and how much the consumer is willing to pay. *See* FTC Study at 3–5.

Personalized algorithmic pricing impacts the prices of many types of goods. A wide range of businesses use the practice, including grocery stores, department stores, health and beauty retailers, home goods and furnishing stores, ride-hailing apps, and rental car companies. *See* FTC Study at 7. Specific examples include Target charging $100 more for a TV on its app based on the consumer's proximity to a Target store, Chris Hrapsky, *The Target App Price Switch: What You Need to Know*, KARE (Jan. 27, 2019),[15] and online booking sites charging $500 more for the same hotel room based on the consumer's home location, Keith A. Spencer, *Hotel Booking Sites Show Higher Prices to Travelers from Bay Area*, SFGate (last updated Feb. 3, 2025).[16]

Algorithmic pricing is difficult for consumers to detect without mandated transparency. Companies largely harvest, aggregate and

---

[15] https://www.kare11.com/article/money/consumer/the-target-app-price-switch-what-you-need-to-know/89-9ef4106a-895d-4522-8a00-c15cff0a0514.

[16] https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php.

analyze personal data outside of consumers' view or control. *See* McClain *et al.*, *supra* (noting that 67 percent of Americans understand little to nothing about what companies are doing with their data). When a company begins setting personalized prices, nothing looks conspicuously different. Companies engaged in personalized algorithmic pricing have said as much explicitly. When Instacart began an undisclosed personalized algorithmic pricing experiment on users by varying grocery prices, an executive remarked in investor materials that "shoppers are not aware that they're in an experiment." 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).[17] Small changes in price per item can be nearly undetectable but, in the aggregate, can have large impacts on consumers. Instacart found it could increase the amount an average family spends on grocery costs by $1,200 per year. *Id.* But without a disclosure about the pricing practice, a consumer who noticed

[17] https://www.consumerreports.org/money/questionable-business-practices/instacart-ai-pricing-experiment-inflating-grocery-bills-a1142182490/.

a higher monthly grocery bill might chalk it up to other inflationary factors such as supply chain issues. This demonstrates both the powerful impact the practice has on consumers and how hard it can be for consumers to detect it.

The result is a commercial practice that is widespread, secretive, and highly material to consumers' transactions. A disclosure mandate in this circumstance is precisely the situation for which *Zauderer* review is warranted.

B. The Act's disclosure is factual.

The Act requires any company that uses an algorithm to set a price based on a consumer's personal data to disclose, "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA." G.B.L. § 349-a(2). This is an accurate description of personalized algorithmic pricing, *see supra* Part II.A, and it is factual because a price either was or was not set this way.

The Act's disclosure is fact, not opinion. "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA" is either true or false. It is also value neutral. The disclosure contains no opinionated value judgments ("You're paying more because this price was set by an

algorithm using your personal data") or charged language ("We surveilled you to raise your prices").

And while there is no "clarity" requirement under *Zauderer*, *see Expressions Hair Design v. Schneiderman*, 877 F.3d 99, 105 (2d Cir. 2017), the Act's terms are facially and contextually clear to consumers, making it unlikely that a reasonable consumer would misread it in a way that makes it non-factual. Each of the key terms in the disclosure has a clear common understanding and refers to a real-world condition. An "algorithm" is "a step-by-step procedure for solving a problem or accomplishing some end," and typically refers to a computational process. *See Algorithm*, Merriam-Webster.com.[18] In the Act's disclosure, the "algorithm" refers to the computational process the company uses to set the price a consumer sees. G.B.L. § 349-a(a). And "personal data" generally means "any information about an individual." Erika McCallister *et al.*, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and

[18] https://www.merriam-webster.com/dictionary/algorithm.

Technology at 2-1 (2010).[19] Putting these terms together, the common understanding of what the company says, through the Act's disclosure, is that "The price of this specific good or service was set by a computational process using information about you." This statement is true if the company uses software that calculates prices based on information about the consumer, and it is false otherwise.

Besides being facially clear, each of these terms is likely to be familiar to a reasonable consumer given the terms' prominence in public discourse. National and local political conversations have been dominated by discussions of pricing, *see, e.g.*, Hannah Stephens & Andre M. Perry, *In Every Corner of the Country, the Middle Class Struggles with Affordability*, Brookings Inst. (Dec. 2, 2025),[20] algorithms, *see, e.g.*, Brown, *supra*, and personal data, *see, e.g.*, Tara Siegel Bernard *et al.*, *Equifax Says Cyberattack May Have Affected 143*

---

[19] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

[20] https://www.brookings.edu/articles/in-every-corner-of-the-country-the-middle-class-struggles-with-affordability/

Million in the U.S., N.Y. Times (Sept. 7, 2017).[21] People understand and frequently refer to "the algorithm" as something that personalizes their experiences in many domains such as shopping, social media, and streaming websites. *See, e.g.*, Aparajita Bhandari & Sara Bimo, *Why's Everyone on TikTok Now? The Algorithmized Self and the Future of Self-Making on Social Media*, Social Media & Society 5 (2022)[22] (indicating broad "hyper-awareness" of "the algorithm"); Dana Mattioli, *Amazon Changed Search Algorithm in Ways That Boost Its Own Products*, Wall St. J. (Sept. 16, 2019)[23]; Wall St. J., *How Spotify's AI-Driven Recommendations Work* (YouTube, Apr. 15, 2023).[24]

And while the common understanding of "personal data" *includes* sensitive personal data, the common understanding of that term is not *limited* to sensitive personal data. The disclosure's wording is clear. If a consumer mistakenly thinks a company is using their sensitive personal data when it isn't, the confusion doesn't come from the disclosure itself,

---

[21] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.
[22] https://journals.sagepub.com/doi/pdf/10.1177/20563051221086241.
[23] https://www.wsj.com/articles/amazon-changed-search-algorithm-in-ways-that-boost-its-own-products-11568645345.
[24] https://www.youtube.com/watch?v=pGntmcy_HX8.

but instead from how hard it is to find out what data the company actually uses. The remedy for a company that does not use sensitive personal data would be for the company to provide additional factual information about the personal data it *does* use. The company could, for instance, link to the part of their existing privacy policy listing the categories of personal data they collect and use. And if the business *does* use sensitive personal data to set a price, the First Amendment is meant to help a concerned consumer to know that information, not hinder it. There is no First Amendment right to hide relevant, true, factual commercial information from consumers.

C. The Act's disclosure is uncontroversial.

The Act's required disclosure is uncontroversial because the truthfulness of its factual assertion is not in dispute. As a general matter, a disclosure's controversiality hinges on whether the factual accuracy of the statement itself is in dispute, not whether it relates to a controversial topic. *See Volokh*, 148 F.4th at 90 ("And though the policies themselves might be controversial, the fact that they are what they are is not."); *see also CompassCare v. Hochul*, 125 F.4th 49, 65 (2d Cir. 2025) (noting that while labor laws related to reproductive health

care might be controversial, "the existence and contents of" the laws are not). Here, the Act only requires a retailer to disclose their use of algorithmic pricing when they have, indeed, "set[] the price of a specific good or service using personalized algorithmic pricing." G.B.L. § 349-a(2). While concerns about personal privacy and fairness might make the practice controversial, *whether* a company is doing it is not controversial at all. A company is either setting a price in this way or it is not.

Consumer skepticism about personalized algorithmic pricing bolsters the government's ability to impose a basic measure of transparency around this practice rather than preempting it. The fact that a commercial practice is controversial is all the more reason to inform a consumer when it is happening so they can choose whether or not to deal with a business engaging in the practice. Transparency mandates have constitutionally addressed hot-button topics such as genetically modified ingredients in food, *e.g.*, *Grocery Mfrs. Ass'n v. Sorrell*, 102 F. Supp. 3d 583 (D. Vt. 2015), abortion-related labor rights, *e.g.*, *CompassCare*, 125 F.4th at 49, and social media content moderation, *e.g.*, *Volokh*, 148 F.4th at 71.

Most recently, in *Volokh*, this Court recognized that laws requiring social media companies to publicly disclose their content moderation policies could be uncontroversial so long as they merely require disclosure of what the policies are, despite the fact that the policies themselves could be controversial. *Volokh*, 148 F.4th at 90. Content moderation of social media has been the subject of protracted litigation, public scrutiny, and legislative attention at both the federal and state levels. *See, e.g.*, *Moody v. NetChoice*, 603 U.S. 707 (2024) (landmark Supreme Court case about regulation of content moderation); Pat de Brún, *Meta's New Content Policies Risk Fueling More Mass Violence and Genocide*, Amnesty International (Feb. 17, 2025) (detailing intense public scrutiny around the effects of content moderation policies).[25] But the controversiality of content moderation does not render the accurate disclosure of policies controversial. *Volokh*, 148 F.4th at 90, 93.

Commercial disclosures about controversial commercial practices can lead to better regulations in a democracy. The Supreme Court has

---

[25] https://www.amnesty.org/en/latest/news/2025/02/meta-new-policy-changes/.

recognized that commercial speech deserves protection specifically *because* it can inform consumer opinion about regulation of commercial practices:

> [I]f [commercial speech] is indispensable to the proper allocation of resources in a free enterprise system, it is also indispensable to the formation of intelligent opinions as to how that system ought to be regulated or altered. Therefore, even if the First Amendment were thought to be primarily an instrument to enlighten public decisionmaking in a democracy, we could not say that the free flow of information does not serve that goal.

Virginia State Bd. of Pharmacy, 425 U.S. at 766. As the Supreme Court has noted, a person's interest in the free flow of commercial information "may be as keen, if not keener by far, than his interest in the day's most urgent political debate." *Id.* at 763–64. Indeed, the affordability of everyday goods is both a consumer and a political issue and today represents one of the most pressing concerns among voters. *See* Lisa Lerer *et al.*, *Voters See a Middle-Class Lifestyle as Drifting Out of Reach, Poll Finds*, N.Y. Times (Jan. 26, 2026).[26]

---

[26] https://www.nytimes.com/2026/01/26/us/politics/affordability-poll.html.

While *NIFLA v. Becerra*, 585 U.S. 755, 768 (2018), signaled that a truthful statement can nonetheless be controversial in some extremely contentious cases involving religious freedom, New York's requirement that the use of personal data-driven algorithms be disclosed does not implicate those concerns at all.

D. The Act's disclosure is similar to others that are widespread and long-standing in data protection laws.

Disclosure requirements like the one in the Act are widespread throughout federal and state law. In other words, they are part of "a longstanding tradition in this country' supported by a 'historical warrant," *CompassCare*, 125 F.4th at 65. Tentpole federal data protection laws contain similar disclosure requirements, such as the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §6502(b)(1), the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681g(c), 1681(f)(1)(C), and the Health Insurance Portability and Accountability Act's Privacy Rule, 45 CFR § 164.520. A variety of state data protection laws contain the same, such as the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100(a), the California Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22575, and the

Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-578(C), among others. This long history of requiring companies to disclose how they use consumers' personal data demonstrates the widespread agreement that individuals have a right to know this information.

Personal data use disclosure mandates are aligned with First Amendment values. The free flow of information about personal data use is essential for consumers to understand the terms of modern commercial transactions and to take steps to protect themselves and others. For example, the CCPA's disclosure requirements help Californians know the real terms on which they are engaging with a business, and COPPA's disclosure requirements help parents protect their kids from privacy invasions.

It would be difficult to find a limiting principle that would justify applying heightened scrutiny to the Act but not these other crucially important data protection regimes. Many businesses would prefer not to disclose the way they collect and process consumers' personal data, as evinced by their constant lobbying against meaningful data protection laws and their push for weak substitutes that keep consumers in the

dark. *See* EPIC & PIRG, *The State of Privacy* 16–21 (Jan. 2025).[27] With news repeatedly featuring headlines about personal data misuse, it would be easy for a business to cast personal data use disclosures in other data protection laws as controversial along the same lines NRF does here, leaving consumers powerless to understand basic information about their commercial transactions. That result would go against the values enshrined in the Court's commercial speech precedent.

III. THERE IS A STRONG GOVERNMENTAL INTEREST IN INFORMING CONSUMERS WHEN PERSONALIZED ALGORITHMIC PRICING OCCURS.

Under *Zauderer*, a law survives First Amendment scrutiny if it is not "unjustified or unduly burdensome." *Zauderer*, 471 U.S. at 651. This Court has consistently characterized this analysis as a "rational-basis review standard." *CompassCare*, 125 F.4th at 64, 67. As such, the state "'has no obligation to produce evidence, or empirical data to sustain . . . rationality.'" *NYSRA,* 556 F.3d at 134 n.23 (quoting *Lewis v. Thompson*, 252 F.3d 567, 582 (2d Cir. 2001)).

---

[27] https://epic.org/wp-content/uploads/2025/04/EPIC-PIRG-State-of-Privacy-2025.pdf.

The Act comfortably satisfies *Zauderer* review. The law serves an interest in informing consumers about a practice material to a key term of a commercial transaction: the price they are offered. Given this interest, the Act is neither over- nor under-inclusive. Pricing transparency is necessary to allow consumers to make informed decisions when engaging in commercial transactions, even when the pricing practice is used to offer a "discount." And far from making the law under-inclusive, the Act's exemptions reduce the disclosure burden in the few cases where transparency does not serve its full purpose.

A. Pricing transparency is necessary for consumers to make informed decisions.

The New York legislature has a legitimate interest in requiring businesses to inform consumers when they use personalized algorithmic pricing. Consumers generally expect that they will pay the same amount for the same goods and services sold in their geographical area. *See* Consumer Reports, *American Experiences Survey: A Nationally Representative Multi-Mode Survey* 8 (2025).[28] When, instead, prices are

---

[28] https://article.images.consumerreports.org/image/upload/v1760040676/prod/content/dam/surveys/Consumer_Reports_AES_September_2025.pdf.

set differently for each consumer based on their personal characteristics, the state has an interest in ensuring consumers are informed. This information enables consumers to make informed decisions about their consumption. Those that wish to avoid personalized algorithmic pricing can only do so when informed of the practice, while others may choose to comparison shop or take measures to protect their privacy. The information also enables self-governance, spurring consumers to educate themselves about personalized algorithmic pricing and its impact on prices and the economy.

Some consumers may reasonably want to avoid purchasing goods and services whose price is set using personalized algorithmic pricing. Informed consumers regularly avoid interactions with companies whose practices they are uncomfortable with. Consumers recently fled TikTok because it began collecting users' precise geolocation information. *See* Aimee Picchi, *TikTok's New Privacy Policy Is Sparking a Backlash. Here's What to Know*, CBS News (Jan. 28, 2026).[29] Similarly, many consumers avoid buying food from companies that use certain

[29] https://www.cbsnews.com/news/tiktok-new-terms-of-service-privacy-geolocation-personal-information/.

ingredients such as artificial sweeteners or preservatives. *See, e.g.*, Cary Funk *et al.*, *Public Perspectives on Food Risks*, Pew Res. Ctr. (Nov. 19, 2018).[30] Some consumers may also want to avoid purchasing from businesses using personalized algorithmic pricing because they would rather buy goods priced the same as everyone else due to fairness or privacy concerns.

Knowledge that a price was set using personalized algorithms should also spur consumers to comparison shop across products or stores. Because individualized pricing introduces greater variety of pricing into the marketplace, the fact that a business is using this pricing practice signals to consumers that other businesses may offer the product to them at a different price. Consumers may check whether businesses that do not use personalized pricing are charging higher or lower prices. They may also check whether other businesses using personalized pricing are charging more or less. By contrast, secret personalized pricing hides from consumers the fact that prices are more

---

[30] https://www.pewresearch.org/science/2018/11/19/public-perspectives-on-food-risks-2/.

variable across businesses, making it less likely that they will comparison shop to find the best price.

Consumers who know about personalized algorithmic pricing may also choose to bolster their privacy practices. Knowing when and where personalized algorithmic pricing happens helps consumers understand which companies have personal data about them. This may lead to consumers exercising their rights to request data correction or deletion under existing privacy laws or using privacy tools to block data collection to see if that might yield different prices.

Informing consumers when personalized algorithmic pricing occurs also helps the public have more informed debates about important topics such as affordability and economic fairness. For example, shedding light on the practice can inform ongoing debates about whether inflation stems from supply chain issues, corporate greed, or other factors. *See, e.g.*, Alina Selyukh, *Are Greedy Companies to Blame for Grocery Inflation? We Looked at the Data*, NPR (Sep. 9, 2024).[31] Transparency can also enable consumers and the public at

---

[31] https://www.npr.org/2024/09/09/nx-s1-5103935/grocery-prices-inflation-corporate-greedflation.

large to better understand the prevalence and impacts of personalized algorithmic pricing, allowing for more informed engagement in the public policy debates about the practice. *See* Angel Carerras *et al.*, Should "Surveillance Pricing" Be Banned?, NPR (Sept. 23, 2025)[32] (describing a debate about the consumer impacts of personalized algorithmic pricing in which both sides agree that consumers and the public lack knowledge about where and when the practice happens).

Consumers clearly want to know when companies are using personalized pricing. The public has expressed outrage after discovering that companies were secretly using or considering using personalized algorithmic pricing, like when reporting revealed that Kroger may be using facial recognition to personalize pricing, *see* Mayu Tobin-Miyaji, *Kroger's Surveillance Pricing Harms Consumers and Raises Prices, With or Without Facial Recognition*, EPIC (Feb. 14, 2025),[33] and when Delta Airlines' president disclosed that the company's technology can determine prices that individuals are willing to pay, Stanley, *supra*. The

---

[32] https://www.npr.org/2025/09/23/nx-s1-5550264/should-surveillance-pricing-be-banned

[33] https://epic.org/krogers-surveillance-pricing-harms-consumers-and-raises-prices-with-or-without-facial-recognition/.

intense consumer backlash to hidden personalized algorithmic pricing underscores the strong consumer expectation that a price offered to them is the same as that offered to other consumers and that the consumer should be informed if that is not the case.

Contrary to NRF's contention, the State's interest in requiring disclosure of personalized algorithmic pricing extends to when the practice is used ostensibly to offer a consumer a discount. There are material differences between traditional discounts and ones set by personalized algorithmic pricing. Traditional discounts enable consumers to gauge whether they are truly getting a "good deal" because they can compare the discount to the normal list price that they and others would otherwise be paying. Personalized algorithmic pricing discounts frustrate this effort by eliminating or undermining the baselines against which consumers can measure their discounts. For instance, if almost all consumers are offered some discount on an item, it is not clear whether any particular consumer is receiving a good deal. A consumer offered a ten percent discount could be subsidizing other consumers' discounts if most others are offered twenty-five percent or more off, or they could be getting a good deal if most others only receive

five percent off. Personalized algorithmic pricing might also be used to set a different *list* price for each consumer, leading them to perceive the same discount price differently due to the different baselines. Some companies are already experimenting with inflating list prices to see whether it increases consumption. Instacart, for instance, showed shoppers at the same grocery location the same sale price for a bottle of ketchup, but showed them different original list prices, potentially affecting the perception of the discount and encouraging more purchases. Katie J. Wells, Lindsay Owens, Angel Han & Alan Smith, *Consumer Reports & Groundwork Collaborative, Same Cart, Different Price: Instacart's Price Experiments Cost Families at Checkout* 12 (2025).[34] It thus matters little whether a company characterizes their personalized pricing as a discount or not—consumers still have an interest in knowing how the price is set.

B. The Act's exceptions are coherent.

The Act's exemptions are limited to situations a company's use of personalized pricing is unlikely to undermine consumer expectations.

---

[34] https://groundworkcollaborative.org/wp-content/uploads/2025/12/Same-Cart-Different-Price.pdf

Specifically, the Act establishes exceptions for (1) insurance providers; (2) financial institutions; and (3) discounts on pre-existing subscriptions. G.B.L. § 349-a(3). In all three circumstances, the interests justifying the disclosure of algorithmic pricing are diminished, providing a rational basis for their exemption. This is starkly different from the law in *NIFLA* which applied only to one "curiously narrow subset of speakers": crisis pregnancy centers. *See NIFLA*, 585 U.S. at 776–78. By contrast, the Act applies to any business in any industry that uses personalized algorithmic pricing with a few narrow and rational exemptions that certainly satisfy *Zauderer* review.

Unlike in other contexts where algorithmic pricing is a new phenomenon enabled by the internet and other technological advances, the use of personal data and algorithms to set personalized rates has long been the standard practice of the insurance industry. The same is true for financial instruments offered by financial institutions like banks and credit unions. Consumers would never expect an insurer to charge the same rates to all their customers, or a bank to offer loans on the same terms to everyone. Highly regulated and widely known

metrics like credit scores exist for the exact purpose of setting individualized prices in these industries.

The credit and insurance industries' use of personal data is already governed by federal law. "[C]redit" and "insurance" are subject to Section 603 of the FCRA, which regulates the use of consumer reports to determine consumers' eligibility and prices. 15 U.S.C. § 1681a(d)(1). The FCRA also has robust transparency requirements, *id.* §§ 1681g(c), 1681(f)(1)(C), diminishing the state's interest in requiring additional disclosures.

The Act's third and final exemption can be explained on a different, but no less rational, basis. Specifically, the Act makes an exception when a price is "offered [1] to a consumer who has an existing subscription-based contract or subscription-based agreement . . . with [the business] and [2] where such price is less than the price for the same good or service set forth in the subscription-based agreement or . . . contract." G.B.L. § 349-a(3)(d). Because the consumer is being offered the same subscription they currently have, but at a lower price than they are currently paying, the consumer has a baseline to compare the proposed discount to, and it is clear that the discount lowers the

price for the consumer. This is in contrast to other situations where a consumer is offered a "discount" but is unable to see the original price, or where the original price is not the price any consumer pays. In the latter circumstances, the offer of a "discount" may be used to manipulate a consumer into making a purchase they were otherwise reluctant to make by convincing them they are getting an unusually good deal, when in reality far greater discounts may be offered to others.

Far from making the Act under-inclusive and unduly burdensome consequently, these exemptions actually serve to reduce unnecessary burden on businesses where possible and to better align the disclosure requirement with the law's justifying governmental interest. To be sure, it may be possible to identify other hypothetical scenarios where New York's disclosure is not necessary to serve the government's interest of informing and protecting consumers that the law does not contain carve-outs for. But *Zauderer*'s rational-basis standard does not require adoption of every exemption possible. The Act's exemptions serve to reduce the burden by not requiring disclosure in the most obvious cases

where such disclosure would not serve the same public interest, and do not render the Act unduly burdensome.

NRF's argument that the exemptions constitute speaker-based discrimination, meriting more exacting scrutiny, is similarly unavailing. Compelled commercial disclosures are inherently speaker- and content-based, and this does not undercut their constitutionality. *See CompassCare*, 125 F.4th at 49. NRF seeks to distinguish this case from other Second Circuit precedents by arguing the exemptions here, unlike in other *Zauderer* cases, treat "similarly situated" businesses differently. But the exempted businesses are *not* similarly situated, since their algorithmic pricing activities pose a substantially diminished threat to the governmental interests served by the Act.

Given the legitimate governmental interest in protecting consumers and preventing their confusion, and the presence of targeted exemptions in cases where such interests are not served, the Act satisfies *Zauderer*'s rational basis review.

CONCLUSION

For the foregoing reasons, *amicus* respectfully urge the Court to affirm the district court's order granting the Defendant's motion to dismiss.

Date: February 17, 2026

/s/ Megan Iorio
Megan Iorio
Tom McBrien
Mayu Tobin-Miyaji
Hayden Davis
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(b)(4) because this brief contains 5824 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point font in Century Schoolbook font.

Signature: *<u>/s/ Megan Iorio</u>* **Date:** February 17, 2026

CERTIFICATE OF SERVICE

I certify that on February 17, 2026, this brief was e-filed through the ACMS of the U.S. Court of Appeals for the Second Circuit. I certify that all participants in the case are registered ACMS users and that service will be accomplished by the ACMS.

Date: February 17, 2026

/s/ Megan Iorio
Megan Iorio
Tom McBrien
Mayu Tobin-Miyaji
Hayden Davis
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center