



March 13, 2026

Co-Chair James Maroney
Co-Chair Roland Lemar
General Law Committee
Connecticut General Assembly
Legislative Office Building, Room 3500
Hartford, CT 06106

Re: S.B. 4 (Legislation to Amend the Connecticut Consumer Data Privacy Act) — *SUPPORT WITH AMENDMENTS*

Dear Chairs Maroney and Lemar,

Consumer Reports writes to support several elements of S.B. 4, legislation to amend the Connecticut Consumer Data Privacy Act, and to recommend certain targeted amendments to improve the bill's consumer protections. In particular, CR supports Sections 1-9, relating to data brokers, Section 12, relating to the definition of publicly available information, Section 15, relating to precise geolocation data, and Section 17, relating to facial recognition technology. CR also writes to share our views on Section 11, relating to algorithmic pricing disclosures, which doesn't go far enough to address consumer harms caused by surveillance pricing.

Sections 1-9 (Universal Data Broker Deletion Mechanism)

CR strongly supports Sections 1-9 of S.B. 4, which seeks to enable consumers to request the deletion of their personal information from all of the state's registered data brokers' records in a single action. This proposal would also require data brokers to report what information they collect on consumers and would impose civil penalties and fines on data brokers who fail to comply with the registration or deletion requirements. This proposal will provide a straightforward, powerful, and critically important tool for protecting the privacy and security of Connecticut residents' personal information.

Data brokerage is a multi-billion-dollar industry centered on collecting and selling people's personal data, typically without their knowledge or explicit consent. It poses a host of significant risks to Connecticut residents. Data brokers amass personal dossiers on virtually every American that include thousands of data points, including extremely granular information about people's behavior online and offline, religious practices and beliefs, physical and mental health conditions, finances, political affiliations, precise geolocation derived from cellphones and connected devices, as well as their inferences about individuals based on this existing data.¹ Some data brokers even collect and sell

¹ See, e.g., Joseph Cox, *The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for \$15*, 404 Media (Aug. 22, 2023),

information about children. This information is then sold and resold, often for marketing but for a variety of other purposes as well, eroding consumers' basic expectation of privacy in the process.²

A few examples of data broker-driven harms include:

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use data brokers to target vulnerable individuals for scams, or otherwise use personal information to cause harm. Some data brokers sell lists of consumers sorted by characteristics like “Rural and Barely Making It,” “Retiring on Empty: Single,” and “Credit Crunched: City Families,” which can be used to target individuals most likely to be susceptible to scams or other predatory products.³ Data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.⁴
- *Predatory use of consumer data.* Data brokers sell data about people who rarely even know the companies even exist—and who have rarely ever affirmatively, expressly consented to this data collection and sale. In some instances, this can result in financially disastrous consequences for consumers. A recent case brought by the Texas Attorney General alleged that Arity, a data broker owned by the insurance company Allstate, secretly harvested information about consumers' driving behaviors (including their precise geolocation data), which it used in some cases to raise consumers' premiums or deny them coverage altogether.⁵ They also sold the driving data to several other insurance companies without consumers' knowledge or consent.
- *Enhanced risks of data breaches.* Data brokers collect trillions of data points on Americans, so they are unsurprisingly a top target for hackers and cyber criminals. Recently, National Public Data, a data broker that specializes in online background checks and fraud prevention services, saw its own data breached, compromising the privacy and security of 2.9 billion consumers whose personal information they trade in, with particular concern for the 170 million

<https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfo-search-transunion/>;

Douglas MacMillan, Data Brokers are Selling Your Secrets. How States are Trying to Stop Them, Wash. Post (Jun. 24, 2019).

<https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-yoursecrets-how-states-are-trying-stop-them/>.

² Big Data, A Big Disappointment for Scoring Consumer Credit Risk, Nat'l Consumer Law Ctr. at 15-16 (Mar. 2014),

<https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>.

³ Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule; request for public comment, (December 3, 2024),

https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

⁴ Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and ‘Publicly Available Information’ Carve-Outs, (October 30, 2023),

<https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs>

⁵ Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025),

<https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf>

individuals across the US, UK and Canada whose sensitive information, including social security number, was exposed.⁶ And location data broker Gravy Analytics, which has claimed to “collect, process and curate” more than 17 billion signals from people’s smartphones every day,⁷ reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.⁸ This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.⁹

S.B. 4 will make it simple for consumers who do not want their information collected, sold, or retained by data brokers to express this preference. First, the bill will require data brokers to register with the Department of Consumer Protection, pay a nominal registration fee, and share basic information about what types of personal information they collect and sell. Then, the Department is required to create a website providing access to a “universal deletion mechanism” that allows consumers, via single request, to delete their personal information from every data broker that has collected it.

This ability to take control of your data with a single click is critical; there are hundreds of data brokers—virtually all unknown to consumers—making the task of deleting one’s information from each broker on a one-by-one basis daunting, if not impossible. Previous Consumer Reports (CR) testing has shown that when privacy laws lack universal ways to manage privacy choices, consumers struggle to use them. For example, in researching the effectiveness of California’s privacy law, CR found examples of data brokers utilizing onerous opt-out requirements that prevented consumers from stopping the sale of their information.¹⁰ For 42.5% of sites tested, at least one of three testers could not even find the broker’s do not sell link.¹¹ About 46% of the time, consumers were left waiting or unsure about the status of their do not sell request, and 52% of the time, the tester was “somewhat dissatisfied” or “very dissatisfied” with the opt-out process.¹²

Based on registration patterns in states with similar laws, Connecticut 's data broker registry will likely include at least 200 registrations, with the potential for 500 or more, similar to California's experience.¹³ A consumer attempting to exercise deletion rights individually would face extreme

⁶ National Public Data breach: What you need to know, (January 31, 2025), <https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535>

⁷ Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf

⁸ Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), <https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/>

⁹ Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S. Military Personnel, (November 2023), <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf>

¹⁰ Maureen Mahoney, California Consumer Privacy Act: Are Consumers’ Rights Protected, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf2.pdf

¹¹ *Id.*

¹² *Id.*

¹³ Privacy Rights Clearinghouse, Registered Data Brokers (as of November 2024), (December 12, 2024), https://public.tableau.com/app/profile/privacy.rights.clearinghouse/viz/RegisteredDataBrokers2024_17340798229480/DataBrokerDatabaseShowingMissing

burdens searching for registered data brokers, navigating complex websites and privacy policies, and managing follow-up communications.¹⁴ During this lengthy process, data brokers continue to buy and sell the consumer's personal information—potentially even to brokers that previously complied with a deletion request. Today, this is an impossible, Sisyphean challenge for Connecticut consumers; but that changes with S.B. 4.

That said, there are several provisions in Sections 1-9 that should be rewritten to enhance clarity or to strengthen consumer protections. The text of this proposal appears to largely pull from California's Delete Act, legislation that first passed in 2023 and was updated in 2025. Notably, the California Delete Act was drafted as an amendment to the CCPA, and therefore uses CCPA's underlying definitions and exemptions. While this approach works in the California context for the most part, Connecticut's underlying privacy law is significantly different than California's, making the process of replicating the California Delete Act unwieldy in a few different ways.

We therefore suggest the following amendments. We have compiled a more detailed redline that implements these and other changes, but by way of example:

- *Remove exemptions from Section 5(b)(5)(A) that do not apply to data brokers.* Several of the exemptions currently provided in the legislation do not map onto data broker activities and therefore create unnecessary ambiguities that could be exploited as loopholes. For instance, Section 5(b)(5)(A)(v) provides that data brokers shall not be required to complete a deletion request if the personal data is reasonably necessary to “provide any product or service specifically requested by such participating consumer.” By definition, data brokers are those that collect and sell to third parties the personal information of consumers with which they have no direct relationship. Therefore, data brokers would never be collecting personal data providing goods or services requested by consumers. This is a CTDPA exemption primarily meant to apply to covered first-party businesses and not data brokers. It should be stricken. The same principle applies for Section 5(b)(5)(A)(vi) and Section 5(b)(5)(A)(vii).
- *Reduce the overall number of exemptions.* Apart from our technical recommendations regarding exemptions described above, we also recommend reducing the overall number of exemptions on consumer protection grounds. Data brokers are incentivized to avail themselves of any possible exemption and to adopt expansive interpretations of exemptions; after all, their business model depends on retaining as much consumer data as possible. As such, the bill's exemptions should be narrowly tailored and should only exclude activities clearly in the public interest or otherwise protected by existing law. For example, it is reasonable for the bill to create narrow exemptions for data brokers solely acting as processors or carrying out legal obligations on behalf of other businesses, or to facilitate fraud prevention or Know Your Customer-type requirements for others. Any such exemptions should be paired with strict purpose limitation language that clarifies that exempted data should be separated or segregated from data used for any other purpose, deleted immediately upon the expiration of the legal or contractual requirement, and only be used for purposes directly related to such exceptions and shall not be used or disclosed for any other purpose.

¹⁴ McDonald, Aleecia M. and Lorrie Faith Cranor. “The Cost of Reading Privacy Policies.” (2009). <https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>

In particular, the drafters should narrow the bill's blanket Fair Credit Reporting Act (FCRA) exemption and remove the Gramm-Leach-Bliley Act (GLBA) entity-level exemption entirely. Many data brokers are hybrid entities, sometimes acting as credit reporting agencies under the FCRA and sometimes acting as marketing data brokers. While it is reasonable for the law to exclude personal information that is actually being used to furnish a credit report under FCRA, when a hybrid entity receives a deletion request, they should be responsible for deleting their marketing data about consumers. The existing text would exempt such entities wholesale, leaving much consumer data unprotected. Likewise, if financial institutions collect and sell information about non-customers without their awareness, they are engaging in the practice of data brokerage and should be regulated as such. By definition, data collected *directly* from consumers by financial institutions is not within the scope of this legislation and therefore a blanket carveout is unnecessary.

- *Prohibit Data Brokers from Individually Verifying Consumer Deletion Requests.* Data brokers should not be allowed to respond to universal deletion requests by contacting consumers to ask for additional verification or further information to complete the deletion request, as is currently contemplated in Section 5(a)(3) and Section 5(b)(1)(B)(i). The entire purpose of a universal deletion mechanism is to reduce the burdens on consumers by managing the verification process up-front — a benefit that would be largely eroded if data brokers were permitted to respond to universal deletion requests with individualized responses for additional information. These provisions should be stricken, which would align S.B. 4 with the California Delete Act.

Assuming these issues are addressed, this bill's approach will massively reduce friction for Connecticut residents seeking to take back control over their personal information.

Section 11 (Algorithmic Pricing Disclosures)

CR applauds the legislature's effort to tackle personalized algorithmic pricing. Personalized pricing, also sometimes referred to as "surveillance pricing," is when a company uses personal data that they've gathered about a consumer—like data about their online search history, their location, the type of device they are using, or inferences about family structure, health conditions, or income—to set the price of a product or determine the discount offered to a consumer. Section 11 requires that companies provide a generic disclosure when they use personalized algorithmic pricing: "THIS PRICE WAS SET BY AN ALGORITHM USING YOUR PERSONAL DATA." A similar requirement was passed into law in New York in 2025.¹⁵

However, in practice this disclosure has limited utility for consumers—they do not know if the company's use of their personal data resulted in a higher or lower price than the average, and they don't know what specific pieces of data about them the company's algorithm considered. Consumers may object, for example, to the use of their data to profile them, or to charge them the most they individually are willing to pay, but may not object to the use of their location to correctly calibrate delivery costs. This generic disclosure does not allow consumers to make those distinctions. The

¹⁵ Algorithmic Pricing Disclosure Act, NY Gen Bus L § 349-a (2025), accessed at <https://law.justia.com/codes/new-york/gbs/article-22-a/349-a/>

disclosure also does not provide sufficient information for researchers who might want to examine these data practices more closely.

Additionally, it appears any reduction specifically for subscription-based products and services is exempt from the disclosure. This is concerning because personalized pricing can functionally be achieved via narrowly targeted personalized discounts, and the practice of fake discounts—where the “list” price is not a real price—is unfortunately a common problem. It is unclear why subscription services should be exempt.

CR encourages committee members to consider changing this disclosure to a prohibition of surveillance pricing. Many states across the U.S. are currently considering bills that prohibit surveillance pricing, and CR believes that is the appropriate policy response.

Section 12 (Publicly Available Information)

CR supports the proposed amendments to the definition of “publicly available information”, which would include important new exclusions, including for 1) consumer profiles compiled from multiple sources of information, 2) information made available for sale, 3) inferences derived from the previous two categories, and 4) the combination of publicly available information with personal information to create new data.

We are sympathetic to the view that scraping the contents of public or government webpages, collecting and arranging personal data derived from those webpages into a comprehensive dossier, and then selling those dossiers to third-parties goes beyond consumers’ reasonable expectations about publicly available information. Information that was originally generated to serve the public interest (e.g. official government records) has been increasingly commodified by entities with commercial ambitions in ways that often run directly counter to the public interest. Companies like Clearview AI have deeply eroded the public trust by scraping billions of photographs of individuals (primarily sourced from publicly available websites) in the service of a product that allows anyone to instantly identify anybody else in real-time without their knowledge or consent. We agree that data brokers that scrape consumers’ personal data in such a manner should, at a minimum, be required to allow consumers to delete it. Such a construct would also allow people to delete commercial data profiles about them that are sold by people search sites, whose unscrupulous business practices can lead to immense risk for individuals and public officials.¹⁶

We also commend the proposed changes to clarify that consumer profiles based on a combination of public and private information are not “publicly available information.” Data brokers often combine publicly available information with non-public information, sometimes further appended with the data broker’s own inferences about the consumer, to create consumer profiles that are then sold to third-parties.¹⁷ These profiles and inferences should not be considered publicly available information

¹⁶ Lily Hay Newman, Wired, Minnesota Shooting Suspect Allegedly Used Data Broker Sites to Find Targets’ Addresses, <https://www.wired.com/story/minnesota-lawmaker-shootings-people-search-data-brokers/>, (June 16, 2025)

¹⁷ Yael Grauer, Vice, What Are ‘Data Brokers,’ and Why Are They Scooping Up Information About You?, (March 27, 2018), <https://www.vice.com/en/article/what-are-data-brokers-and-how-to-stop-my-private-data-collection/>

just because they may have been created in part from publicly available information—especially when they are being sold to third-parties without the awareness or consent of consumers.

Section 15 (Precise Geolocation Information)

Consumer Reports also strongly supports the proposal to ban the sale of consumer’s precise geolocation data. Geolocation can be incredibly useful for pro-consumer applications such as turn-by-turn directions and finding a nearby restaurant; however, all too often this information is secretly collected and shared by dozens if not hundreds of ad networks and data brokers with whom consumers have no relationship or even awareness. This leads to many of the same consumer harms as described above in the data brokers section.

Unsurprisingly, the advertising industry that profits off this predatory use of consumer data strongly opposes threats to their ill-gotten gains. They offer a number of misleading arguments about why these protections are not needed or are unprecedented. But ultimately businesses do not need to purchase Connecticut residents precise geolocation data in order to effectively advertise. And most of the large companies that traffic in location data already have to be compliant with the protections included in S.B. 4 due to the passage of similar laws elsewhere, including in Oregon, Maryland, and most recently, Virginia. Several other states, including California, Massachusetts, Vermont, Maine, and Washington are considering similar protections this year.

We offer some additional context on some of the advertising industry’s key arguments here:

- *“CTDPA already protects precise geolocation data.”*

Opt-in frameworks, like the one currently in CTDPA, are not robust enough to prevent businesses from selling location data behind consumers’ backs. While it is true that businesses must obtain opt-in consent to process location data under CTDPA, in practice many businesses require you to consent to the sale of your location data as a condition of using the service. In other words, they are not required to obtain separate consent for functionally necessary data collection (e.g. a weather app collecting location to provide an accurate forecast) versus unnecessary secondary sharing (e.g. a weather app selling location to data brokers). Instead, consumers are often presented with a single take-it-or-leave-it consent box that they have to complete if they want to use the product. This type of coercive structure fails to meaningfully protect consumers. Instead of relying on a flimsy pretext of informed “consent,” the law should simply ban harmful practices, like the sale of precise geolocation data.

- *“S.B. 4 will prevent consumers from receiving desired location-based services, like geotargeted coupons.”*

A ban on sale of precise geolocation data would not stop consumers from receiving desired location-based services, such as turn-by-turn directions, ads for local businesses, or coupons. Under this bill, businesses are still free to collect consumers’ location data, with clear, affirmative consent, to advertise to them — they just can’t sell that data to other businesses. Furthermore, businesses that wish to buy or sell consumers’ location information for

advertising purposes can ultimately still do so, albeit in a more privacy-protecting way. Precise geolocation is defined in CTDPA as information that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet — close enough to identify someone’s home address. Instead, businesses could still leverage data at the town, city, or zipcode level. For example, advertisers could advertise based on a consumer’s general location, such as “New Haven area.”

- *“S.B. 4 ignores the very valuable role that geolocation data plays in anti-fraud and law enforcement functions.”*

Nothing in this bill prevents anti-fraud or law enforcement functions. CTDPA already includes a number of exemptions for anti-fraud and law enforcement, including that “nothing in this chapter shall be construed to restrict a controller’s or processor’s ability to... [p]revent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity.” And once again, this bill is about the commercial sale of location data, not the collection of it. Anti-fraud entities and law enforcement are free to lawfully collect precise geolocation, as well as to leverage it for their own purposes.

- *“S.B. 4 will burden low-income consumers. Monetizing user data is critical to the advertising-supported ecosystem that makes many apps free to users.”*

Free iPhone apps that secretly sell consumers’ location data are not a serious cost-of-living issue, while the actual costs to consumers of the unfettered sale of their location data can be severe. Aside from the risks of identity theft, stalking, or predatory marketing described above, businesses are increasingly seeking to use information like location data as an input into “surveillance pricing” algorithms. These systems use extensive data-driven profiling to assess consumers’ personal situations so that they can charge them closer to their maximum willingness to pay and commercial location data brokers are a key cog in that machine.

Ultimately, some types of data are simply too sensitive to allow commercial entities to buy and sell. Granular data about our everyday comings and goings — which reveals the location of our homes, friends’ homes, places of worship, political causes we support, medical services we seek out, and more — is clearly one of those.

Section 17 (Facial Recognition Technology)

Finally, Consumer Reports appreciates the proposal in Section 17 to place guardrails around how controllers can use facial recognition technology for the purposes of preventing fraud, security incidents, and identity theft. The proposal would ensure that controllers can only use facial recognition for these purposes when matching images or video to a database maintained “exclusively by the controller.” Requiring businesses to build their own databases, rather than relying on those created by third-party vendors, will theoretically limit the number of consumers implicated in any given search. There is a significant difference between search parameters that allow “1-to-all” matching (e.g. a globalized database of non-consensually scraped photographs by bad actors like Clearview AI) and “1-to-few” matching (e.g. a database of known shoplifters or registered employees). This should help

mitigate some of the most privacy-eroding uses of the technology (e.g. affirmatively identifying every single entrant to a physical location via facial recognition).

At the same time, it is worth noting that other high-profile misuses of facial recognition in the retail context would not have been constrained by the policies contemplated here. For example, in 2023 the FTC banned Rite Aid from using facial recognition for surveillance purposes despite Rite Aid allegedly maintaining its own photo enrollment database.¹⁸ In that case, Rite Aid failed to put into place reasonable guardrails regarding the creation of its database, resulting in the use of persistently low-quality images that led to erroneous matches. Rite Aid also failed to adequately train its employees on how to responsibly use the system.

So while the use of facial recognition clearly calls for a more comprehensive approach than is considered in this amendment (though the underlying law does at least require businesses to collect opt-in consent prior to collecting faceprints), we do believe this is a step forward in the interim.

For the above reasons, we are proud to support S.B. 4 and urge the Legislature to approve it.

Sincerely,

Matt Schwartz
Senior Policy Analyst
Consumer Reports

Grace Gedye
Senior Policy Analyst
Consumer Reports

¹⁸ Federal Trade Commission, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards, (December 19, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>