March 4, 2026

Connecticut Joint Committee on General Law
Legislative Office Building, Room 3500
Hartford, CT 06106

RE: SB 4 "An Act Concerning Consumer Privacy" (Oppose, Unless Amended)

Dear Chair Maroney, Chair Lemar, and Members of the Joint Committee on General Law:

On behalf of the Computer & Communications Industry Association (CCIA), I write to raise several concerns regarding SB 4. CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms.[1]

CCIA strongly supports consumer data protection and understands that Connecticut residents are rightfully concerned about keeping their data safeguarded properly. CCIA also appreciates lawmakers' continued efforts to allow innovation to thrive while preserving meaningful consumer protection.

However, several provisions of SB 4 would place Connecticut businesses at a competitive disadvantage without meaningfully improving consumer privacy. Accordingly, CCIA recommends the following amendments to the bill:

§ 1(7) – "Data broker"

This definition should be limited to entities that do not have a direct relationship with the consumer, following California and Vermont's example.[2] The Connecticut Data Privacy Act (CDPA) already regulates entities that have a direct relationship with the consumer,[3] and as noted below, conflicts with SB 4 in several respects. A bill regulating data brokers should not subject other businesses to inconsistent obligations.

§ 1(9) – "Data service provider"

This definition should be removed, and the obligations conferred upon data service providers should be transferred to data brokers. Entities that process data on behalf of data brokers are not necessarily data brokers themselves, and should not be subject to data broker specific requirements.

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Cal. Civ. Code § 1798.99.80(c) (West 2024), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.99.80.&lawCode=CIV; Vt. Stat. Ann. tit. 9, § 2430(4)(A) (2018), https://legislature.vermont.gov/statutes/section/09/062/02430.
[3] Conn. Gen. Stat. § 42-515(7)(C) (2024), https://www.cga.ct.gov/2024/sup/chap_743jj.htm.

§ 11(a)(7) – "Personalized algorithmic pricing"

To address the fundamental flaws with the overly broad definition and blanket prohibition included in SB 4, while ensuring transparency and properly addressing the issues the bill seeks to target, CCIA urges adopting the following key amendments:

1. **Target the Harm**: Narrow the definition of "personalized algorithmic pricing" to focus exclusively on individualized price increases. This protects legitimate uses of data, such as personalized promotions and loyalty programs, and avoids imposing higher overhead on retailers operating on the margins, and consequently higher costs for the very consumers the bill seeks to protect.
2. **Establish a "Baseline Price"**: Define a clear reference point (the price generally available to the public in a region) so that businesses and regulators can objectively determine when a price has actually been increased for a specific user.
3. **Clarify Disclosures**: Amend the required disclosure language to: "**THIS PRICE WAS INCREASED BY AN ALGORITHM USING YOUR PERSONAL DATA.**" This ensures transparency is reserved for instances where the consumer is actually being charged more, rather than when they are receiving a discount.

These amendments would maintain affordability protections for consumers while preserving their ability to use promotions, discounts, and loyalty programs. They would also avoid penalizing sellers for incorporating regional shipping costs into their prices or increasing prices in response to rising input costs.

§ 11(b)(3)(A) – Exceptions

Under this exception, language should be added to exempt price deviations arising from health insurance pricing from the restrictions on personalized algorithmic pricing.

§ 12(35)(B)(iv) – "Publicly available information"

The carve-out for "inferences generated" from information used to create profiles on publicly available websites or information made available for sale should be changed to "personal data inferences generated." This change would avoid scoping in all algorithms derived from third-party sets or used to weight models based on such information.

§ 12(35)(B)(viii)(II) – "Publicly available information"

The exception for "where the consumer has maintained a reasonable expectation of privacy in such information, including, but not limited to, by restricting such information to a specific audience" is unnecessary and should be removed. The definition of "publicly available information" is itself limited to information that a controller or processor "has a reasonable basis to believe that the consumer has lawfully made available to the general public", which already encompasses the exception. Adding this exception forces covered entities to operate under two different definitions of "publicly available information," which creates regulatory conflict without meaningfully enhancing consumer privacy.

§ 13(a)(2) – Employment opportunities

This section assigns controllers a specific duty when using automated processing "that results in the provision or denial by the controller to the consumer of any employment opportunity." However, this provision contradicts the definition of "consumer" in Section 12(8), which explicitly excludes "an individual acting in a commercial or employment context or as an employee." Employee privacy should be regulated separately from consumer privacy , as employees and consumers are subject to fundamentally different sets of potential privacy harms. Doing so would also help avoid contradictory regulations like the ones above.

§ 14(a)(6)(E) – Employment opportunities

For the same reasons as above, data subject rights that specifically pertain to employment should be regulated separately from consumer privacy rights. Accordingly, CCIA recommends that such rights be instituted in a law where they will not contradict the definition of "consumer."

§ 15(a)(3) – Precise geolocation data

The rule that "No controller shall sell, share or transfer, or allow any other person to access, precise geolocation data" is far more restrictive than in other state laws. Oregon, for instance, bans only the sale of such data.[4] Consumers may wish to consent to having such data shared, and controllers may process such data without revealing it publicly. CCIA therefore recommends creating exceptions to this prohibition for sharing such data with processors, direct transfers of such data, or where the consumer consents to such data being shared.

§ 16(a)(2) – Precise geolocation data

As noted above, processors' obligations regarding precise geolocation data should be removed and such duties should instead be assigned to controllers. Processors, by definition, can only process data as controllers instruct. Entities with greater autonomy are controllers, not processors.

§ 17(a)(2)(A)(i) – Facial recognition technology

This restriction on the use of facial recognition technology (FRT) for security purposes rules out many security operations that do not jeopardize user privacy. Not all covered entities will have the means to maintain their own FRT database and may have to outsource FRT-based image comparisons to third parties. Moreover, the law already requires that controllers who process biometrics or other sensitive data prepare DPIAs. Accordingly, this section should permit controllers to check their FRT images obtained for security purposes against databases maintained by other entities.

[4] Oregon Consumer Privacy Act, Or. Rev. Stat. § 646A.578(2)(d)(B) (2025). *See* https://olis.oregonlegislature.gov/liz/2025R1/Downloads/MeasureDocument/HB2008/Enrolled (since enacted as an amendment to the above law).

§ 17(a)(2)(B) – Facial recognition technology

This subsection should be removed. While well-intentioned, requiring "the controller, processor, or consumer health controller to… [e]nable a consumer to readily determine whether the consumer is included in the database" requires controllers to maintain personally identifying information (PII) regarding individuals in its FRT databases. This undermines consumer privacy by forcing covered entities to institute a means of identifying such individuals. It also lets malicious actors discern whether a given individual is in a given database. The requirement to process a deletion request will also be an infeasible timeline for many covered entities.

* * * * *

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Respectfully submitted,

Kyle J. Sepe
State Policy Manager, Northeast Region
Computer & Communications Industry Association