OLR Bill Analysis

sSB 4

AN ACT CONCERNING CONSUMER PRIVACY AND PROTECTION.

TABLE OF CONTENTS:

SUMMARY

This bill makes various unrelated changes related to consumer privacy and protection, as described in the section-by-section analysis

below.

EFFECTIVE DATE: October 1, 2026

§§ 1-9 — DATA BROKERS

Requires data brokers to register with DCP; establishes a deletion mechanism program for consumers to request that data brokers delete their personal data; requires data brokers to check the program once every 45 days; creates a civil penalty of up to $5,000 per day per violation

Licensing (§ 2)

The bill generally requires data brokers who sell or license brokered data in the state on or after January 1, 2027, to be actively registered with the Department of Consumer Protection (DCP).

These data brokers must submit to DCP, as the commissioner requires, an application for an initial registration with a $600 initial registration fee. The initial registration expires on December 31 of the year it is issued and may be renewed for successive one-year terms. The renewal application must be made in the same way as an initial application and with a $600 renewal fee. All these fees are deposited in the General Fund.

All applications must disclose:

1. the applicant's name, mailing address, and an actively monitored email address and telephone number;

2. the applicant's primary website address;

3. a publicly accessible webpage address on the applicant's primary website that (a) does not make use of any dark pattern (a user interface designed with the substantial effect of subverting or impairing user autonomy, decision-making, or choice) and (b) details how a consumer may exercise each of their rights under the Connecticut Data Privacy Act (CTDPA; see BACKGROUND);

4. whether the applicant collects (a) minors' personal data, or (b) consumers' precise geolocation data or reproductive or sexual health data;

5. the measures the applicant must take to ensure that no personal data is sold or licensed in violation the bill's data broker provisions and the CTDPA;

6. if, and to what extent, the applicant or any of its subsidiaries is regulated under the (a) Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.), (b) Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and its regulations, (c) Insurance Data Security Law (CGS § 38a-38), or (d) privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services (45 C.F.R. Parts 160 and 164);

7. for renewals submitted on or after July 1, 2028, the statement the applicant most recently posted on a publicly accessible webpage on their primary website as required by the bill (see § 6 below);

8. for renewals submitted on or after July 1, 2030, (a) whether the applicant has undergone an audit as required by the bill (see § 5 below), and (b) if so, the most recent audit report and related materials; and

9. any other information the DCP commissioner requires.

The bill also allows DCP to approve and renew a data broker registration under the terms of an agreement between the department and the Nationwide Multistate Licensing System.

Prohibition on Selling Personal Data (§ 3)

The bill prohibits data brokers from selling or licensing any personal data in violation of the bill's data broker provisions and the CTDPA. Each registered data broker must have a privacy policy which, at a minimum, includes measures to ensure compliance with this prohibition.

Deletion Mechanism (§ 5)

The bill requires the DCP commissioner, by January 1, 2027, to establish an accessible deletion mechanism program. The program must have an accessible deletion mechanism that:

1. allows a consumer for whom a registered data broker has collected personal data, or his or her authorized agent, to (a) submit a free deletion request, in a commissioner-prescribed verifiable way and in any language a consumer speaks, to have all registered data brokers and data service providers delete their personal data, and (b) specifically exclude one or more registered data brokers, and all applicable data service providers, from the deletion request;

2. allows a consumer, or his or her authorized agent, to (a) securely submit additional personal data to help process the deletion request, (b) check the deletion request status, and (c) submit updates to the verified deletion request no more than once in any 45-day period;

3. allows a registered data broker to determine whether a consumer, or his or her authorized agent, has specifically excluded the broker and the broker's data service providers from the deletion request or any update;

4. prohibits a registered data broker that accesses the deletion mechanism for determining whether it has been excluded to access any additional personal data through the deletion mechanism;

5. is readily accessible and usable by consumers with disabilities;

6. incorporates reasonable security safeguards, including administrative, physical, and technical safeguards, to protect consumers' personal data from any unauthorized use, disclosure, access, destruction, or modification through the deletion mechanism; and

7. provides, in a readily understandable way to consumers, (a) a description of what is considered personal data and may be deleted if requested, (b) an explanation of the deletion request process, and (c) a description of the actions the bill requires for brokers to delete personal data.

Unverified Request

Beginning on February 15, 2027, the DCP commissioner or his authorized agent must verify that the consumer or the consumer's authorized agent actually submitted the deletion request or update. If the commissioner or his authorized agent cannot verify the request or update, then the commissioner or authorized agent must specify that all registered data brokers and their data service providers that are not specifically excluded from the unverified deletion request or update (1) may retain any personal data on the consumer, and (2) must process the unverified deletion request or update as an exercise of the consumer's rights under the CTDPA to opt-out of personal data processes for certain purposes, such as targeted advertisement.

Broker Deletion Requirements

Beginning February 15, 2027, each registered data broker must access the accessible deletion mechanism at least once every 45 days to examine each deletion request or update to determine whether the broker and its data service providers are specifically excluded from that request or update.

For each verified deletion request or update that does not specifically exclude the broker and its data service providers, the broker must generally delete any personal data it maintains on the consumer and direct all data service providers with any of the consumer's personal data held on the broker's behalf to also do so.

For each unverified deletion request or update that does not specifically exclude the broker and its data service providers, the broker must (1) retain any personal data the broker has about the consumer, and (2) process the unverified deletion request or update, and direct all of its data service providers to process the unverified request or update, as an exercise of the consumer's rights under the CTDPA to opt-out of personal data processes for certain purposes.

The bill also generally requires brokers to, at least once every 45 days after it first deletes a participating consumer's personal data, to repeat the bill's required actions for a verified request or update. Brokers do

not have to do this if:

1. the broker verifies that the participating consumer or his or her authorized agent has submitted a verified update to a verified deletion request; and

2. the verified update specifically excludes the broker and all its data service providers from the updated deletion request.

Allowable DCP Fee

The bill allows the DCP commissioner to impose a fee on each registered data broker that accesses the accessible deletion mechanism to perform its duties after a deletion request or update. The commissioner determines the fee amount, but it must not exceed the cost of providing the service. Collected fees must be deposited in the General Fund.

Subsequently Acquired Data Prohibition

The bill generally prohibits, beginning February 15, 2027, registered data brokers and their data service provider that delete a participating consumer's personal data from maintaining, using, or disclosing any personal data they subsequently acquire about the participating consumer.

Excepted Circumstances

Under the bill, a registered data broker who maintains a participating consumer's personal data and its data service provider do not have to delete a consumer's personal data, and may maintain, use, or disclose it, when it is reasonably necessary to:

1. comply with any federal, state, or municipal law, ordinance, or regulation;

2. comply with any civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by any federal, state, municipal, or other governmental authority;

3. cooperate with any law enforcement agency about any conduct

or activity that the registered data broker or data service provider reasonably and in good faith believes may violate any federal, state, or municipal law, ordinance, or regulation;

4. investigate, establish, exercise, prepare for, or defend any legal claim;

5. provide any product or service the participating consumer specifically requests;

6. perform any contract where the participating consumer is a party, including fulfilling written warranty terms;

7. take any step at the participating consumer's request to enter a contract;

8. take any immediate step to protect any interest that is essential for the life or physical safety of the participating consumer or another person;

9. prevent, detect, protect against, or respond to any security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity; preserve the integrity or security of any system; or investigate, report, or prosecute those responsible for these actions;

10. engage in any public or peer-reviewed scientific or statistical research in the public interest that follows all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines, or has a similar independent oversight entity that determines, that (a) maintaining the participating consumer's personal data is likely to provide substantial benefits that do not exclusively benefit the registered data broker or data service provider, (b) the expected benefits of the research outweigh the privacy risks, and (c) the broker or data service provider has implemented reasonable safeguards to mitigate privacy risks associated with the research;

11. help any other person in performing any obligation imposed the

bill's data broker provisions;

12. do internal research to develop, improve, or repair any product, service, or technology;

13. carry out a product recall;

14. identify and repair any technical error that impairs existing or intended functionality; or

15. perform internal operations that are reasonably aligned with the expectations the participating consumer had, or reasonably anticipated, based on the consumer's existing relationship with the broker.

The bill generally prohibits registered data brokers or their data service providers from maintaining, using, or disclosing the participating consumer's personal data for any other purpose.

Audit

The bill generally requires, beginning July 1, 2030, and every three years after, registered data brokers to:

1. retain an independent auditor to audit their books to determine their compliance with the bill's deletion mechanism requirements, prepare an audit report disclosing the results, and submit the report and any associated materials to the broker, and

2. maintain each audit report and associated materials for at least six years from when they are submitted to the broker.

The bill generally requires a registered data broker to submit the audit report and the materials to DCP within five business days after the department sends notice to the broker it must do so.

DCP Contract for Implementation

The bill allows the DCP commissioner to contract with one or more public or private entities for any services needed to implement these provisions or to run the accessible deletion mechanism program.

DCP Website (§ 4)

The bill requires the DCP commissioner to make, and periodically update, a webpage on the department's website disclosing: (1) for each registered data broker, the information in the broker's most recent approved application; and (2) the accessible deletion mechanism established by the commissioner.

Data Broker Website Disclosures (§ 6)

The bill generally requires, by July 1, 2028, each business that was a registered data broker during the prior calendar year to annually post, in commissioner-prescribed way and on a publicly accessible webpage on the business's primary website, a statement disclosing the following information:

1. the total number of deletion requests, including any updates, that the business accessed the prior year and that did not specifically exclude the business and its data service providers;

2. the total number of deletion requests to which the business responded by (a) deleting personal data; (b) retaining personal data; or (c) deleting some and retaining other personal data; and

3. if the business responded to one or more deletion requests by retaining personal data, the total number of the deletion requests for which it kept personal data based on the (a) excepted circumstances listed above or (b) exemptions listed below.

Exemptions (§ 7)

The bill's data broker provisions do not apply to:

1. a consumer reporting agency, a person who furnishes information to a consumer reporting agency, or a user of a consumer report, to the extent that they engage in activities that are subject to regulation under the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.;

2. a financial institution, an affiliate, or a nonaffiliated third party, to the extent they engage in activities that are subject to

regulation under Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., and its regulations;

3. a business that collects information about a consumer if the consumer is or was (a) in a contractual relationship with the business, (b) an investor in or donor to the business, or (c) in any relationship with the business that is like the relationships above;

4. a business that performs services or acts as the agent for a business where the consumer has a previous relationship, as described above; or

5. a business collecting data used for purposes regulated certain federally listed chemicals (21 U.S.C. § 830).

The bill's data broker provisions should not be construed to prohibit an unregistered data broker from engaging in any sale or licensing of brokered personal data if the sale or licensing exclusively involves:

1. publicly available information that (a) is about a consumer's business or profession, (b) is sold or licensed as part of a service that provides alerts for health or safety purposes, or (c) is lawfully available from any federal, state, or local government record, unless the information is collated and combined to create a consumer profile that is made available to a user of a publicly accessible website, or used to generate inferences related to consumers;

2. giving digital access to any (a) journal, book, periodical, newspaper, magazine, or news media, or (b) educational, academic, or instructional work;

3. developing or maintaining an electronic commerce service or software;

4. providing directory assistance or information services as, or on behalf of, a telecommunications carrier; or

5. a one-time or occasional disposition of the assets of a business, or

any portion of a business, as part of a transfer of control over the business's assets that is not part of the business's ordinary conduct.

Regulations (§ 8)

The bill allows the DCP commissioner to adopt regulations to implement these provisions.

Penalty (§ 9)

The bill allows the DCP commissioner, after giving notice and holding a hearing following the Uniform Administrative Procedure Act, to impose a civil penalty of up to $5,000 per day for each violation of the bill's data broker provisions. Any civil penalty collected is deposited into the General Fund.

§ 10 — NEW CAR TARIFF COST ESTIMATE

Requires new car manufacturers to disclose in a clear, conspicuous, and understandable way, the tariff cost estimate for the new car

The bill requires new car manufacturers that ship new cars to Connecticut to stick a label on the windshield or side window showing in a clear, conspicuous, and readily understandable way the new car's tariff cost estimate. A "tariff cost estimate" is an estimate of any price increase on the disclosure label caused, directly or indirectly, by any federally imposed tariff, including any tariff on steel, aluminum, or other item used to manufacture, assemble, or distribute a new car.

Under the bill, a manufacturer (1) may satisfy this label requirement by including the tariff cost estimate as part of the disclosure label stuck on the new car and (2) that violates this provision may be fined up to $1,000.

§ 11 — PERSONALIZED ALGORITHMIC PRICING

Generally (1) requires online businesses that use personalized algorithmic pricing to increase the price of consumer goods or services to specifically disclose that and (2) prohibits businesses from using an electronic pricing label that uses personalized algorithmic pricing for in-person transactions; deems violations CUTPA violations

Disclosure for Online Price Increases

Under the bill, any person (individual or entity) doing business in the

state that uses personalized algorithmic pricing to increase the price for a specific consumer good or service (primarily for personal, family, or household purposes) as part of an online transaction generally must include the following disclosure on their online advertisement, promotion, label, statement, display, image, offer, or announcement: "THIS PRICE WAS INCREASED BY AN ALGORITHM USING YOUR PERSONAL DATA." This disclosure must be readily visible to the average consumer.

This warning is for goods or services to be sold, leased, exchanged, or provided as part of an online transaction by anyone who advertises or promotes the price online, labels a consumer good price online, or publishes an online statement, display, image, offer, or announcement disclosing the price. Under the bill, "personalized algorithmic pricing" means using automated computational processes that use a series of rules to set a price for a consumer good or service based on their personal data.

Prohibition for In-Person Sales

The bill generally prohibits any person doing business in the state from using an electronic pricing label that uses personalized algorithmic pricing to increase a consumer good's price for an in-person transaction. An "electronic pricing label" is any electronic display in a retail establishment that is part of digital network used to automatically display and update a consumer good's pricing information.

Exemptions

Under the bill, these provisions do not apply to:

1. any person required to be credentialed or authorized to operate under the state's insurance laws;

2. any financial institution or affiliate, to the extent they are subject to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq.; or

3. any bank, holding company, or out-of-state bank or holding company that establishes an office in the state and is subject to the banking commissioner's supervision.

Penalty

Under the bill, violations of these provisions are deemed a Connecticut Unfair Trade Practices Act (CUTPA) violation (see BACKGROUND).

§§ 12-17 — CTDPA

Modifies what is considered publicly available information for CTDPA purposes; requires certain signage and privacy policies before controllers can use facial recognition technology, among other requirements; gives consumers the right to correct incorrect information a third-party provides if denied employment based on automated profiling; prohibits controllers from selling, sharing, transferring, or allowing anyone else to access precise geolocation data

Publicly Available Information (§ 12)

Under existing law, publicly available information is not "personal data" and is, therefore, not subject to the CTDPA (see BACKGROUND).

The bill modifies what is considered publicly available information. Under current law, as amended by PA 25-113, which will go into effect July 1, 2026, "publicly available information" is information that (1) is lawfully available through federal, state, or municipal government records or widely distributed media or (2) a controller has a reasonable basis to believe the consumer has lawfully made available to the general public or has been lawfully made available to the general public from widely distributed media.

The bill expands what is considered publicly available information:

1. by removing the requirement that governmental records be lawfully made available and instead just requires their availability, and

2. to include all data from a widely distributed media, regardless of whether the information was made available lawfully, rather than only when the controller reasonably believes information has been lawfully made available from widely distributed media.

Current law has various exemptions to what is considered publicly available data, including biometric data that can be associated with a specific consumer and was collected without the consumer's consent.

The bill instead exempts biometric data a business collects about a consumer without his or her knowledge.

The bill also adds the following exemptions:

1. information that is collated and combined to create a consumer profile and made available to a user of a publicly accessible website;

2. information made available for sale;

3. inference generated from the information about the consumer profile and sales, as described above;

4. obscene visual depictions;

5. personal data created by combining any personal data with any publicly available information;

6. genetic data, unless the consumer makes it publicly available;

7. information a consumer provides on a publicly accessible website or online service where the (a) website or online service is made available to the general public and (b) consumer has a reasonable expectation of privacy in the information, including by restricting the information to a specific audience; or

8. intimate images or synthetically created intimate images known to be nonconsensual, as defined under the state's unlawful dissemination of an intimate or synthetic image laws.

Facial Recognition Technology (§§ 12 & 17)

Regardless of the law limiting the CTDPA's applicability to restrict a controller's ability to (1) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; (2) preserve the integrity or security of systems; or (3) investigate, report, or prosecute those responsible for these actions, the bill prohibits controllers, processors, or consumer health data controllers from using facial recognition

technology for these purposes unless it meets certain conditions. They must:

1. exclusively use the facial recognition technology to match still images or video to a database they exclusively control and

2. post clearly legible signs at each entrance where the technology is used, other than entrances where access is restricted to authorized employees.

The signs must (1) alert consumers entering the premises that facial recognition technology is being used and (2) include a conspicuous hyperlink or quick response (QR) code that directs consumers to the privacy policy the controller, processor, or consumer health data controller maintains.

Privacy Policy. The bill requires each privacy policy to require the controller, processor, or consumer health data controller to:

1. enable a consumer to (a) readily determine they are in the database and (b) if so, submit to the controller, processor, or consumer health data controller a written request to be removed from it; and

2. within 15 days after receiving a removal request, (a) either grant or deny it, and (b) send a written notice of the decision and its reasoning to the requesting consumer, and if the request was denied, the contact information for the attorney general's office.

Denial of Employment Based on Profiling (§§ 13 & 14)

Under the CTDPA, consumers have the right to opt out of the processing of personal data for certain purposes, including if the data was processed to profile them to make automated legal decisions or those with similarly significant effects.

By law, these include allowing the consumer to (1) question the result; (2) be notified of the reason for the outcome; (3) review the data used for processing; and (4) correct any incorrect personal data,

depending on the data's nature and the processing purposes, if it was used for housing matters.

Depending on the nature of the data and the processing purposes, the bill expands this to profiling decisions resulting in a denial of an employment opportunity. In these cases, the bill allows the consumer to:

1. be notified if any personal data processed for the profiling was submitted by a third party,

2. correct any incorrect personal data submitted by a third party processed for profiling purposes, and

3. have the profiling decision reevaluated based on the corrected personal data.

The bill also specifies that the CTDPA's list of exempted organizations and entities are not excused from performing the controller's duties in responding to a consumer's rights under a denial of employment based on profiling. They must do this if the organization or entity processes the consumer's personal data to generate an automated decision that ultimately results in denying a consumer an employment opportunity.

By law, the CTDPA exempts from its requirements various entities, including state and local governments, nonprofits (federally tax exempt 501(c)(3), (4), (6), or (12) organizations), and higher education institutions.

Precise Geolocation (§§ 15 & 16)

The bill prohibits controllers and processors from selling, sharing, transferring, or allowing anyone else to access precise geolocation data.

Under existing law, certain controllers are generally prohibited from collecting a minor's precise geolocation and must, when collecting this data, give the minor a signal that the collection is happening. It is also considered sensitive data that a controller may not process without

consumer consent or, if the consumer is younger than age 13, the minor's parent or guardian's consent.

§ 18 — AUTOMATIC LICENSE PLATE READERS

Starting October 1, 2026, prohibits DOT, DMV, and law enforcement agencies from entering or renewing contracts with ALPR users unless the user agrees to certain conditions (for example, not selling ALPR information or allowing unauthorized entities access to this information)

Starting October 1, 2026, the bill prohibits the Department of Transportation (DOT), Department of Motor Vehicles (DMV), and law enforcement agencies from entering into or renewing any contract with automatic license plate reader (ALPR) users (those who own or operate or have access to ALPR information) unless the user agrees to certain conditions.

Under the bill, an ALPR is a mobile or fixed electronic device that can record data on, or take a photograph or video of, a vehicle or its license plate. "Law enforcement agency" means the attorney general's office, the chief state's attorney's office, State Police, or any municipal police department.

Under the bill, ALPR users must agree not to:

1. sell ALPR information (information that the ALPR gathers, or that is created through an analysis of the information the ALPR gathers);

2. share or transfer ALPR information to anyone other than DOT, DMV, or a law enforcement agency;

3. allow anyone besides these entities to access the information unless the user (the one who owns or operates or has access to ALPR information) is required by a judicial warrant or valid court order or for exigent circumstances (unforeseeable circumstances posing imminent threat to public health or safety, including if reasonably believed necessary to prevent physical harm to a person, the destruction of evidence, or a suspect's escape, but does not include certain immigration investigative or enforcement activities); or

4. share, transfer, or allow access to the information if the user reasonably believes it may be used (a) to investigate any suspected immigration violation or assist any immigration enforcement activity; (b) to investigate any suspected, or prosecute any alleged, activity, including any protected health care activity, that is legal in Connecticut; or (c) for any effort to identify, or impose any civil or criminal liability on, anyone just for engaging in constitutionally protected activity (for example freedom of speech, peaceful assembly, or petitioning the government).

The bill makes ALPR information confidential and not disclosable under the Freedom of Information Act. It also allows the (1) attorney general to institute proceedings to enforce this provision and (2) court to grant appropriate relief, including preliminary, temporary, or permanent injunctive relief.

Under the bill, "protected health care activity" means (1) seeking, providing, or receiving reproductive health care services or gender-affirming health care services, and (2) helping others who are seeking, providing, or receiving these services, including by providing information, transportation, lodging, or material support to these them.

BACKGROUND

CUTPA

By law, CUTPA prohibits businesses from engaging in unfair and deceptive acts or practices. It allows the DCP commissioner, under specified procedures, to issue regulations defining an unfair trade practice, investigate complaints, issue cease and desist orders, order restitution in cases involving less than $10,000, impose civil penalties of up to $5,000, enter into consent agreements, ask the attorney general to seek injunctive relief, and accept voluntary statements of compliance. It also allows individuals to sue. Courts may issue restraining orders; award actual and punitive damages, costs, and reasonable attorney's fees; and impose civil penalties of up to $5,000 for willful violations and up to $25,000 for a restraining order violation.

CTDPA

The CTDPA, among other things:

1. sets a framework for controlling and processing personal data,

2. sets responsibilities and privacy protection standards for data controllers (those that determine the purpose and means of processing personal data) and processors (those that process data for a controller),

3. generally applies to individuals (1) doing business in Connecticut or producing products or services targeted to Connecticut residents and (2) controlling or processing personal data of numbers of consumers above specified thresholds during the previous calendar year.

Related Bills

sSB 5, favorably reported by the General Law Committee, requires those who use an automated decision process in making an employment-related decision to provide certain disclosures and a written notice with certain information, with different requirements for adverse decisions. It also prohibits an employer from using this kind of automated process in a way that causes the employer to discriminate against someone based on certain traits (for example, their race, religion, or gender identity)

sSB 435, favorably reported by the Labor and Public Employees Committee, sets limitations and requirements for using an automated employment-related decision process. It also makes various changes related to artificial intelligence (AI), including making the use of AI a subject of collective bargaining for public sector employees.

sHB 5449, favorably reported by the Judiciary Committee, restricts public agencies or law enforcement agencies from using ALPR systems, or using or sharing ALPR data, except for listed reasons, and requires related policies and reporting.

sSB 5552, favorably reported by the Government Administration and

Elections Committee, imposes requirements for ALPR contracts related to how the entity operating the system may store or use the information, among other things.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 16 Nay 5 (03/16/2026)