Senate

General Assembly

File No. 285

February Session, 2026

Substitute Senate Bill No. 4

Senate, April 1, 2026

The Committee on General Law reported through SEN. MARONEY of the 14th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

AN ACT CONCERNING CONSUMER PRIVACY AND PROTECTION.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective October 1, 2026*) As used in this section and sections 2 to 9, inclusive, of this act, unless the context otherwise requires:

(1) "Accessible deletion mechanism" means the mechanism established pursuant to subsection (a) of section 5 of this act;

(2) "Applicant" means any data broker that submits an application for an initial registration, or for a registration renewal, under subsection (b) of section 2 of this act;

(3) "Brokered personal data" means any personal data that a data broker obtains from a third party and categorizes or organizes for the purpose of enabling the data broker to sell or license such personal data to another person;

(4) "Business" (A) means (i) any person who regularly engages in

commercial activities for the purpose of generating income, (ii) any bank, Connecticut credit union, federal credit union, out-of-state bank, out-of-state trust company or out-of-state credit union, as such terms are defined in section 36a-2 of the general statutes, and (iii) any other person who controls, is controlled by or is under common control with any person described in subparagraph (A)(i) or (A)(ii) of this subdivision, and (B) does not include any body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state;

(5) "Commissioner" means the Commissioner of Consumer Protection;

(6) "Consumer" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(7) "Data broker" means any business or, if such business is not an individual, any portion of such business that sells or licenses brokered personal data to another person;

(8) "Data service provider" means any person who maintains personal data on behalf of a registered data broker;

(9) "Deletion request" means any request submitted by or on behalf of a consumer under subparagraph (A) of subdivision (1) of subsection (a) of section 5 of this act;

(10) "Department" means the Department of Consumer Protection;

(11) "License" (A) means to grant access to, or distribute, brokered personal data in exchange for consideration, and (B) does not include using any personal data for the sole benefit of the person who provided such personal data if such person maintains control over the use of such personal data;

(12) "Minor" means any consumer who is younger than eighteen years of age;

(13) "Participating consumer" means any consumer who submits a verified deletion request either directly or through an authorized agent;

(14) "Person" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(15) "Personal data" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(16) "Registered data broker" means any data broker that is actively registered as a data broker in accordance with the provisions of section 2 of this act; and

(17) "Unregistered data broker" means any data broker that is not actively registered as a data broker in accordance with the provisions of section 2 of this act.

Sec. 2. (NEW) (*Effective October 1, 2026*) (a) Except as provided in section 7 of this act, no data broker shall sell or license brokered personal data in this state on or after January 1, 2027, unless the data broker is actively registered with the Department of Consumer Protection in accordance with the provisions of this section.

(b) Except as provided in subsection (d) of this section and section 7 of this act, a data broker that intends to sell or license brokered personal data in this state shall submit to the Department of Consumer Protection, in a form and manner prescribed by the Commissioner of Consumer Protection, an application for an initial registration as a data broker. Each application for an initial registration as a data broker shall be accompanied by an initial registration fee in the amount of six hundred dollars. Each initial registration issued pursuant to this subsection shall expire on December thirty-first of the year in which such initial registration was issued, and may be renewed for successive one-year terms upon submission of a registration renewal application made in the manner set forth in this subsection for an initial application and payment of a registration renewal fee in the amount of six hundred dollars. All fees collected under this subsection shall be deposited in the

General Fund.

(c) Except as provided in subsection (d) of this section, each application submitted to the Department of Consumer Protection under subsection (b) of this section shall disclose: (1) The applicant's name, mailing address and an actively monitored electronic mail address and telephone number; (2) the address of the applicant's primary Internet web site; (3) the address of a publicly accessible Internet web page on the applicant's primary Internet web site that (A) does not make use of any dark pattern, as defined in section 42-515 of the general statutes, as amended by this act, and (B) details how a consumer may exercise each of the rights afforded to the consumer under subsection (a) of section 42-518 of the general statutes, as amended by this act; (4) whether the applicant collects (A) minors' personal data, or (B) consumers' precise geolocation data or reproductive or sexual health data, as such terms are defined in section 42-515 of the general statutes, as amended by this act; (5) the measures the applicant will take to ensure that no personal data is sold or licensed in violation of the provisions of sections 1 to 9, inclusive, of this act or sections 42-515 to 42-526, inclusive, of the general statutes, as amended by this act; (6) whether, and to what extent, the applicant or any of its subsidiaries is regulated under (A) the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time, (B) Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., and the regulations adopted thereunder, as said act and such regulations may be amended from time to time, (C) section 38a-38 of the general statutes, or (D) the privacy, security and breach notification rules issued by the United States Department of Health and Human Services, 45 CFR Parts 160 and 164, as amended from time to time; (7) for a registration renewal application submitted on or after July 1, 2028, the statement the applicant most recently posted on a publicly accessible Internet web page on such applicant's primary Internet web site pursuant to section 6 of this act; (8) for a registration renewal application submitted on or after July 1, 2030, (A) whether the applicant has undergone an audit pursuant to subparagraph (A)(i) of subdivision (1) of subsection (d) of section 5 of this act, and (B) if the applicant has undergone an audit pursuant to subparagraph (A)(i) of subdivision (1) of subsection (d) of

section 5 of this act, the most recent year for which the applicant submitted an audit report and the materials associated therewith to the department pursuant to subdivision (2) of subsection (d) of section 5 of this act; and (9) any other information the Commissioner of Consumer Protection requires for the purposes of this section.

(d) The Department of Consumer Protection may approve and renew an application for registration as a data broker in accordance with the terms of an agreement between the department and the Nationwide Multistate Licensing System.

Sec. 3. (NEW) (*Effective October 1, 2026*) No data broker shall sell or license any personal data in violation of the provisions of sections 1 to 9, inclusive, of this act or sections 42-515 to 42-526, inclusive, of the general statutes, as amended by this act. Each registered data broker shall establish a privacy policy which, at a minimum, shall include measures to ensure that such registered data broker does not sell or license any personal data in violation of the provisions of sections 1 to 9, inclusive, of this act or sections 42-515 to 42-526, inclusive, of the general statutes, as amended by this act.

Sec. 4. (NEW) (*Effective October 1, 2026*) The Commissioner of Consumer Protection shall establish, and periodically update, an Internet web page on the Department of Consumer Protection's Internet web site disclosing: (1) For each registered data broker, the information required under subsection (c) of section 2 of this act that was included in the application such registered data broker most recently submitted, and the department most recently approved for such registered data broker, under subsection (b) of section 2 of this act; and (2) the accessible deletion mechanism established by the commissioner pursuant to subsection (a) of section 5 of this act.

Sec. 5. (NEW) (*Effective October 1, 2026*) (a) Not later than January 1, 2027, the Commissioner of Consumer Protection shall establish an accessible deletion mechanism program. As part of the accessible deletion mechanism program, the commissioner shall establish an accessible deletion mechanism that:

(1) Enables a consumer, or the consumer's authorized agent, to (A) submit a deletion request, in a verifiable form and manner prescribed by the commissioner, without charge to the consumer or such authorized agent and in any language spoken by a consumer for whom a registered data broker has collected personal data, that all registered data brokers and data service providers delete the consumer's personal data, and (B) specifically exclude one or more registered data brokers, and all data service providers for such registered data broker or brokers, from the consumer's deletion request;

(2) Enables a consumer, or the consumer's authorized agent, to (A) securely submit additional personal data, in a form and manner prescribed by the commissioner, to aid in processing the consumer's deletion request, (B) determine the status of the consumer's deletion request, and (C) not more frequently than once during any forty-five-day period, submit an update to the participating consumer's verified deletion request in a verifiable form and manner prescribed by the commissioner, without charge to such participating consumer or such participating consumer's authorized agent and in any language spoken by a consumer for whom a registered data broker has collected personal data;

(3) Enables a registered data broker to determine whether a consumer, or the consumer's authorized agent, has specifically excluded the registered data broker, and all data service providers for such registered data broker, from the consumer's deletion request or any update thereto;

(4) Does not enable a registered data broker that accesses the accessible deletion mechanism for the purposes set forth in subdivision (3) of this subsection to access any additional personal data by way of such accessible deletion mechanism;

(5) Is readily accessible and usable by consumers with disabilities;

(6) Incorporates reasonable security safeguards, including, but not limited to, administrative, physical and technical safeguards, to protect

consumers' personal data from any unauthorized use, disclosure, access, destruction or modification by way of the accessible deletion mechanism; and

(7) Provides, in a manner that is readily understandable by consumers, (A) a description of what constitutes personal data and therefore may be subject to a deletion request, (B) an explanation of the processes for a consumer, or the consumer's authorized agent, to submit and update a deletion request, and (C) a description of the actions required under subsections (b) and (c) of this section.

(b) On and after February 15, 2027, and except as provided in section 7 of this act, the Commissioner of Consumer Protection, or the commissioner's authorized agent, shall:

(1) Verify that the consumer, or the consumer's authorized agent, who purportedly submitted a deletion request or update thereto actually submitted such deletion request or update; and

(2) If the commissioner, or the commissioner's authorized agent, cannot verify that the consumer, or the consumer's authorized agent, who purportedly submitted a deletion request or update thereto actually submitted such deletion request or update, specify that all registered data brokers, and all data service providers for such registered data brokers, that are not specifically excluded from such unverified deletion request or such unverified update (A) may retain any personal data such registered data brokers and data service providers maintain concerning such consumer, and (B) shall process such unverified deletion request or such unverified update as an exercise of such consumer's right under subparagraph (B) of subdivision (5) of subsection (a) of section 42-518 of the general statutes, as amended by this act.

(c) (1) On and after February 15, 2027, and except as provided in section 7 of this act, each registered data broker shall access the accessible deletion mechanism at least once every forty-five days to:

(A) Examine each deletion request or update thereto to determine whether such registered data broker, and all data service providers for such registered data broker, are specifically excluded from such deletion request or update; and

(B) (i) For each verified deletion request or verified update thereto that does not specifically exclude such registered data broker, and all data service providers for such registered data broker, and subject to the exceptions set forth in subdivision (5) of this subsection, delete any personal data such registered data broker maintains concerning the participating consumer and direct all data service providers that maintain any personal data concerning the participating consumer on behalf of such registered data broker to delete such personal data; or

(ii) For each unverified deletion request or unverified update thereto that does not specifically exclude such registered data broker, and all data service providers for such registered data broker, (I) retain any personal data such registered data broker maintains concerning the consumer, and (II) process such unverified deletion request or such unverified update, and direct all data service providers for such registered data broker to process such unverified deletion request or such unverified update, as an exercise of the consumer's right under subparagraph (B) of subdivision (5) of subsection (a) of section 42-518 of the general statutes, as amended by this act.

(2) At least once every forty-five days after a registered data broker first deletes a participating consumer's personal data pursuant to subparagraph (B)(i) of subdivision (1) of this subsection, repeat the actions required under subparagraph (B)(i) of subdivision (1) of this subsection unless:

(A) Such registered data broker verifies that the participating consumer, or the participating consumer's authorized agent, has submitted a verified update to a verified deletion request such participating consumer or authorized agent previously submitted to the accessible deletion mechanism; and

(B) Such verified update specifically excludes such registered data broker and all data service providers for such registered data broker from the verified updated deletion request.

(3) The Commissioner of Consumer Protection may impose a fee on each registered data broker that accesses the accessible deletion mechanism for the purposes of performing such registered data broker's duties under subdivisions (1) and (2) of this subsection. Such fee shall be in an amount determined by the commissioner, but shall not exceed the cost of providing such access. All fees collected under this subdivision shall be deposited in the General Fund.

(4) On and after February 15, 2027, and except as provided in subdivision (5) of this subsection, no registered data broker, and no data service provider for such registered data broker, that deletes a participating consumer's personal data pursuant to subparagraph (B)(i) of subdivision (1) of this subsection or subdivision (2) of this subsection shall maintain, use or disclose any personal data such registered data broker or data service provider subsequently acquires concerning the participating consumer.

(5) (A) No registered data broker who maintains a participating consumer's personal data, and no data service provider for such registered data broker, shall be required to delete the participating consumer's personal data, and may maintain, use or disclose such consumer's personal data, to the extent that maintaining, using or disclosing such participating consumer's personal data is reasonably necessary to (i) comply with any federal, state or municipal law, ordinance or regulation, (ii) comply with any civil, criminal or regulatory inquiry, investigation, subpoena or summons by any federal, state, municipal or other governmental authority, (iii) cooperate with any law enforcement agency concerning any conduct or activity that such registered data broker or data service provider reasonably and in good faith believes may violate any federal, state or municipal law, ordinance or regulation, (iv) investigate, establish, exercise, prepare for or defend any legal claim, (v) provide any product or service specifically

requested by such participating consumer, (vi) perform pursuant to any contract to which such participating consumer is a party, including, but not limited to, by fulfilling the terms of a written warranty, (vii) take any step at the request of such participating consumer prior to entering into a contract, (viii) take any immediate step to protect any interest that is essential for the life or physical safety of such participating consumer or another individual, (ix) 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 any such action, (x) engage in any public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board, or a similar independent oversight entity, that determines that (I) maintaining such participating consumer's personal data is likely to provide substantial benefits that do not exclusively accrue to such registered data broker or data service provider, (II) the expected benefits of such research outweigh the privacy risks, and (III) such registered data broker or data service provider has implemented reasonable safeguards to mitigate any privacy risk associated with such research, (xi) assist any other person in performing any obligation imposed under sections 1 to 9, inclusive, of this act, (xii) conduct internal research to develop, improve or repair any product, service or technology, (xiii) effectuate a product recall, (xiv) identify and repair any technical error that impairs existing or intended functionality, or (xv) perform internal operations that are reasonably aligned with the expectations such participating consumer had, or reasonably anticipated, based on such participating consumer's existing relationship with such registered data broker.

(B) Except as provided in section 7 of this act, no registered data broker, or data service provider for such registered data broker, that maintains, uses or discloses a participating consumer's personal data for any purpose set forth in subparagraph (A) of this subdivision shall maintain, use or disclose the participating consumer's personal data for any other purpose.

(d) (1) Except as provided in section 7 of this act, not later than July 1, 2030, and triennially thereafter, each registered data broker shall, at the expense of such registered data broker, (A) retain an independent auditor to (i) audit the books of such registered data broker to determine whether such registered data broker is in compliance with the provisions of subsection (c) of this section, (ii) prepare an audit report disclosing the results of such audit, and (iii) submit such audit report, and any materials associated therewith, to such registered data broker, and (B) maintain each audit report, and any materials associated therewith, that are submitted to such registered data broker pursuant to subparagraph (A)(iii) of this subdivision for a period of at least six years beginning on the date on which such audit report and materials are submitted to such registered data broker.

(2) Except as provided in section 7 of this act, a registered data broker shall submit an audit report and the materials described in subparagraph (A)(iii) of subdivision (1) of this subsection to the Department of Consumer Protection, in a form and manner prescribed by the Commissioner of Consumer Protection, not later than five business days after the department sends notice to the registered data broker disclosing that the department requires such registered data broker to submit such audit report and materials to the department.

(e) The Commissioner of Consumer Protection may enter into a contract with one or more public or private entities for any services necessary to implement the provisions of subsections (a) to (d), inclusive, of this section or to administer the accessible deletion mechanism program established pursuant to subsection (a) of this section.

Sec. 6. (NEW) (*Effective October 1, 2026*) Except as provided in section 7 of this act, not later than July 1, 2028, and annually thereafter, each business that was a registered data broker during the preceding calendar year shall post, in a form and manner prescribed by the Commissioner of Consumer Protection and on a publicly accessible Internet web page on such business's primary Internet web site, a

statement disclosing the following information:

(1) The total number of deletion requests, inclusive of any updates thereto, that such business accessed during the preceding calendar year and that did not specifically exclude such business and all data service providers for such business;

(2) The total number of deletion requests described in subdivision (1) of this section to which such business responded by:

(A) Deleting personal data;

(B) Retaining personal data; or

(C) Deleting and retaining personal data; and

(3) If such business responded to one or more deletion requests described in subdivision (1) of this section by retaining personal data, the total number of such deletion requests for which such business retained personal data:

(A) On the basis of an exception set forth in subdivision (5) of subsection (c) of section 5 of this act; or

(B) On the basis of an exemption set forth in section 7 of this act.

Sec. 7. (NEW) (*Effective October 1, 2026*) (a) The provisions of sections 1 to 9, inclusive, of this act shall not apply to: (1) A consumer reporting agency, as defined in 15 USC 1681a(f), as amended from time to time, a person who furnishes information to a consumer reporting agency, as provided in 15 USC 1681s-2, as amended from time to time, or a user of a consumer report, as defined in 15 USC 1681a(d), as amended from time to time, to the extent that the consumer reporting agency, person or user engages in activities that are subject to regulation under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (2) a financial institution, an affiliate or a nonaffiliated third party, as such terms are defined in 15 USC 6809, as amended from time to time, to the extent that the financial institution, affiliate or nonaffiliated third

party engages in activities that are subject to regulation under Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., and the regulations adopted thereunder, as said act and such regulations may be amended from time to time; (3) a business that collects information concerning a consumer if the consumer is or was (A) in a contractual relationship with the business, (B) an investor in the business, (C) a donor to the business, or (D) in any relationship with the business that is similar to the relationships described in subparagraphs (A) to (C), inclusive, of this subdivision; (4) a business that performs services for, or is acting as an agent or otherwise on behalf of, a business described in subdivision (3) of this subsection; or (5) a business collecting data used for purposes of the regulation of listed chemicals as set forth in 21 USC 830, as amended from time to time.

(b) No provision of sections 1 to 9, inclusive, of this act shall be construed to prohibit an unregistered data broker from engaging in any sale or licensing of brokered personal data if such sale or licensing exclusively involves: (1) Publicly available information that (A) concerns 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 such information is (i) collated and combined to create a consumer profile that is made available to a user of a publicly accessible Internet web site for compensation or free of charge, or (ii) used to generate inferences with respect to consumers; (2) providing 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 directory 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 assets of the business that is not part of the ordinary conduct of such business or portion of such business.

Sec. 8. (NEW) (*Effective October 1, 2026*) The Commissioner of

Consumer Protection may adopt regulations, in accordance with the provisions of chapter 54 of the general statutes, to implement the provisions of sections 2 to 7, inclusive, of this act.

Sec. 9. (NEW) (*Effective October 1, 2026*) The Commissioner of Consumer Protection, after providing notice and conducting a hearing in accordance with the provisions of chapter 54 of the general statutes, may impose a civil penalty of not more than five thousand dollars per day for each violation of any provision of sections 2 to 7, inclusive, of this act. Any civil penalties collected under this section shall be deposited in the General Fund.

Sec. 10. (NEW) (*Effective October 1, 2026*) (a) As used in this section:

(1) "Disclosure label" means the label that a manufacturer is required to affix to a new automobile manufactured or imported by the manufacturer pursuant to 15 USC 1232, as amended from time to time;

(2) "Manufacturer" has the same meaning as provided in 15 USC 1231, as amended from time to time;

(3) "New automobile" has the same meaning as provided in 15 USC 1231, as amended from time to time;

(4) "New motor vehicle dealer" means a new motor vehicle dealer licensed in accordance with section 14-52 of the general statutes; and

(5) "Tariff cost estimate" means an estimate of any increase in the price or prices listed on the disclosure label caused, directly or indirectly, by any tariff imposed by the federal government, including, but not limited to, any such tariff imposed on steel, aluminum or any other item used to manufacture, assemble or distribute a new automobile.

(b) (1) A manufacturer that ships a new automobile to a new motor vehicle dealer in the state on or after October 1, 2026, shall affix to the windshield or side window of the new automobile a label disclosing, in a clear, conspicuous and readily understandable manner, the tariff cost

estimate for such new automobile.

(2) A manufacturer may satisfy the requirements established in subdivision (1) of this subsection by including the tariff cost estimate for the new automobile as part of the disclosure label affixed to the new automobile.

(c) A manufacturer that violates any provision of subsection (b) of this section shall be fined not more than one thousand dollars.

Sec. 11. (NEW) (*Effective October 1, 2026*) (a) As used in this section:

(1) "Algorithm" means any computational automated process that uses a set of rules to define a sequence of operations;

(2) "Consumer" means any individual who is physically present in the state;

(3) "Consumer good" means any article that is purchased, leased, exchanged or received primarily for personal, family or household purposes;

(4) "Consumer service" means any service that is purchased, leased, exchanged or received primarily for personal, family or household purposes;

(5) "Controller" has the same meaning as provided in section 42-515 of the general statutes, as amended by this act;

(6) "Electronic pricing label" means any electronic display that (A) is located within a retail establishment, (B) is part of a digital network, and (C) is used to automatically display and update pricing information for a consumer good offered for sale within the retail establishment;

(7) "Person" means any individual, association, corporation, limited liability company, partnership, trust or other legal entity;

(8) "Personalized algorithmic pricing" means any process that uses an algorithm to establish the price for a consumer good or consumer

service based in whole or in part on personal data; and

(9) "Personal data" (A) means any information that is linked or reasonably linkable to an identified or identifiable consumer or a device linked to such consumer, and (B) does not include (i) data that cannot reasonably be used to infer information about or otherwise be linked to an identified or identifiable consumer or a device linked to such consumer if the controller that possesses such data (I) takes reasonable measures to ensure that such data cannot be associated with a consumer, (II) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (III) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (B)(i)(I) and (B)(i)(II) of this subdivision, or (ii) any information that (I) is lawfully made available through federal, state or municipal government records or widely distributed media, and (II) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

(b) (1) Except as provided in subsection (d) of this section, any person doing business in the state who uses personalized algorithmic pricing to increase the price for a specific consumer good or consumer service to be sold, leased, exchanged or provided as part of an online transaction, and who directly or indirectly advertises or promotes such price online, labels a consumer good with such price online or publishes an online statement, display, image, offer or announcement disclosing such price, shall include in such online advertisement, promotion, label, statement, display, image, offer or announcement the following disclosure: "THIS PRICE WAS INCREASED BY AN ALGORITHM USING YOUR PERSONAL DATA".

(2) The disclosure required under subdivision (1) of this subsection shall be readily visible to the average consumer.

(c) Except as provided in subsection (d) of this section, no person doing business in the state shall use an electronic pricing label that uses personalized algorithmic pricing to increase the price for a specific consumer good to be sold as part of an in-person transaction.

(d) The provisions of subsections (b) and (c) of this section shall not apply to:

(1) Any person licensed, authorized to operate or registered, or required to be licensed, authorized to operate or registered, pursuant to the insurance laws of this state;

(2) Any financial institution or affiliate thereof, as such terms are defined in 15 USC 6809, as amended from time to time, to the extent such financial institution or affiliate is subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., as amended from time to time; or

(3) Any bank, holding company or out-of-state bank, as such terms are defined in section 36a-2 of the general statutes, or out-of-state holding company, as defined in section 36a-410 of the general statutes, that directly or indirectly establishes an office in the state and is subject to the supervision of, or regulation by, the Banking Commissioner pursuant to title 36a of the general statutes.

(e) Any violation of the provisions of subsection (b) or (c) of this section shall constitute an unfair or deceptive trade practice for the purposes of subsection (a) of section 42-110b of the general statutes.

Sec. 12. Section 42-515 of the 2026 supplement to the general statutes, as amended by section 5 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

As used in this section and sections 42-516 to 42-526, inclusive, unless the context otherwise requires:

(1) "Abortion" means terminating a pregnancy for any purpose other than producing a live birth.

(2) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this subdivision, "control" and "controlled" mean (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting

security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) the power to exercise controlling influence over the management of a company.

(3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 42-518, as amended by this act, is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

(4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data are generated to identify a specific individual.

(5) "Business associate" has the same meaning as provided in HIPAA.

(6) "Child" has the same meaning as provided in COPPA.

(7) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include (A) acceptance of general or broad terms of use or a similar document that contains descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.

(8) "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial [or

employment**]** context, under the direction of an employer or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit organization or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit organization or government agency.

(9) "Consumer health data" means any personal data that a controller uses to identify a consumer's physical or mental health condition, diagnosis or status, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data.

(10) "Consumer health data controller" means any controller that, alone or jointly with others, determines the purpose and means of processing consumer health data.

(11) "Controller" means a person who, alone or jointly with others, determines the purpose and means of processing personal data.

(12) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

(13) "Covered entity" has the same meaning as provided in HIPAA.

(14) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

(15) "Decision that produces any legal or similarly significant effect" means any decision made by the controller, or on behalf of the controller, that results in the provision or denial by the controller of any financial or lending service, any housing, any insurance, any education enrollment or opportunity, any criminal justice, any employment

opportunity or any health care service.

(16) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(17) "Facial recognition technology" means any technology that (A) analyzes facial features in still images or video, and (B) is used (i) to assign a unique persistent identifier, or (ii) to uniquely and personally identify a specific individual.

[(17)**]** (18) "Gender-affirming health care services" has the same meaning as provided in section **[**52-571n**]** 52-571m.

[(18)**]** (19) "Gender-affirming health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

[(19)**]** (20) "Geofence" means any technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data or any other form of location detection, or any combination of such coordinates, connectivity, data, identification or other form of location detection, to establish a virtual boundary.

[(20)**]** (21) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

[(21)**]** (22) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

[(22)**]** (23) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

[(23)**]** (24) "Mental health facility" means any health care facility in which at least seventy per cent of the health care services provided in such facility are mental health services.

[(24)**]** (25) "Neural data" means any information that is generated by measuring the activity of an individual's central nervous system.

[(25)**]** (26) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.

[(26)**]** (27) "Person" means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity.

[(27)**]** (28) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

[(28)**]** (29) "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

[(29)**]** (30) "Process" and "processing" mean any operation or set of operations performed, whether by manual or automated means, on

personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

[(30)**]** (31) "Processor" means a person who processes personal data on behalf of a controller.

[(31)**]** (32) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

[(32)**]** (33) "Protected health information" has the same meaning as provided in HIPAA.

[(33)**]** (34) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

[(34)**]** (35) "Publicly available information" (A) means information that (i) is **[**lawfully**]** made available **[**from**]** through federal, state or **[**municipal**]** local government records or to the general public from widely distributed media, or (ii) a controller or processor, or an affiliate of a controller or processor, has a reasonable basis to believe **[**(I) a**]** that the consumer has lawfully made available to the general public, **[**or (II) has been lawfully made available to the general public from widely distributed media,**]** and (B) does not include any (i) biometric data **[**that can be associated with a specific**]** about a consumer **[**and were**]** collected by a business without the consumer's **[**consent**]** knowledge, (ii) information that is collated and combined to create a consumer profile that is made available to a user of a publicly accessible Internet web site for compensation or free of charge, (iii) information that is made available for sale, (iv) inference generated from the information described in subparagraph (B)(ii) or (B)(iii) of this subdivision, (v)

obscene visual depiction, as such term is used in 18 USC 1460, as amended from time to time, (vi) personal data that is created by combining any information described in subdivision (28) of this section with any information described in subparagraph (A) of this subdivision, (vii) genetic data, unless such genetic data is made publicly available by the consumer, (viii) information provided by a consumer on a publicly accessible Internet web site or online service (I) which Internet web site or online service is made available to the general public for compensation or free of charge, and (II) 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, (ix) intimate image, as such term is used in section 53a-189c, known to be nonconsensual, or (x) intimate synthetically created image, as such term is used in section 53a-189d, known to be nonconsensual.

[(35)**]** (36) "Reproductive or sexual health care" means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being, including, but not limited to, any such service or product rendered or provided concerning (A) an individual health condition, status, disease, diagnosis, diagnostic test or treatment, (B) a social, psychological, behavioral or medical intervention, (C) a surgery or procedure, including, but not limited to, an abortion, (D) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion, (E) a bodily function, vital sign or symptom, (F) a measurement of a bodily function, vital sign or symptom, or (G) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

[(36)**]** (37) "Reproductive or sexual health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

[(37)**]** (38) "Reproductive or sexual health facility" means any health care facility in which at least seventy per cent of the health care-related services or products rendered or provided in such facility are

reproductive or sexual health care.

[(38)**]** (39) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal data to an affiliate of the controller, (D) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, (E) the disclosure of personal data that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience, or (F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets.

[(39)**]** (40) "Sensitive data" means personal data that includes (A) data revealing (i) racial or ethnic origin, (ii) religious beliefs, (iii) a mental or physical health condition, diagnosis, disability or treatment, (iv) sex life, sexual orientation or status as nonbinary or transgender, or (v) citizenship or immigration status, (B) consumer health data, (C) genetic or biometric data or information derived therefrom, (D) personal data collected from an individual the controller has actual knowledge, or wilfully disregards, is a child, (E) data concerning an individual's status as a victim of crime, as defined in section 1-1k, (F) **[**precise geolocation data, (G)**]** neural data, **[**(H)**]** (G) a consumer's financial account number, financial account log-in information or credit card or debit card number that, in combination with any required access or security code, password or credential, would allow access to a consumer's financial account, or **[**(I)**]** (H) government-issued identification number, including, but not limited to, Social Security number, passport number, state identification card number or driver's license number, that

applicable law does not require to be publicly displayed.

[(40)**]** (41) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include (A) advertisements based on activities within a controller's own Internet web sites or online applications, (B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer's request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach.

[(41)**]** (42) "Third party" means a person, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller.

[(42)**]** (43) "Trade secret" has the same meaning as provided in section 35-51.

Sec. 13. Subsection (a) of section 42-517 of the 2026 supplement to the general statutes, as amended by section 7 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) (1) The provisions of sections 42-515 to 42-525, inclusive, as amended by this act, do not apply to any: **[**(1)**]** (A) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; **[**(2)**]** (B) person who has entered into a contract with any body, authority, board, bureau, commission, district or agency described in subparagraph (A) of this subdivision **[**(1) of this subsection**]** while such person is processing consumer health data on behalf of such body, authority, board, bureau, commission, district or agency pursuant to such contract; **[**(3)**]** (C) nonprofit organization; **[**(4)**]** (D) candidate committee, national committee, party committee or

political committee, as such terms are defined in section 9-601; **[**(5)**]** (E) institution of higher education; **[**(6)**]** (F) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; **[**(7)**]** (G) covered entity or business associate, as defined in 45 CFR 160.103; **[**(8)**]** (H) tribal nation government organization; **[**(9)**]** (I) air carrier, as defined in 49 USC 40102, as amended from time to time, and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time; **[**(10)**]** (J) insurer, as defined in section 38a-1, or its affiliate, fraternal benefit society, within the meaning of section 38a-595, health carrier, as defined in section 38a-591a, insurance-support organization, as defined in section 38a-976, or insurance agent or insurance producer, as such terms are defined in section 38a-702a; **[**(11)**]** (K) bank, Connecticut credit union, federal credit union, out-of-state bank or out-of-state credit union, or any affiliate or subsidiary thereof, as such terms are defined in section 36a-2, that **[**(A)**]** (i) is only and directly engaged in financial activities as described in 12 USC 1843(k), **[**(B)**]** (ii) is regulated and examined by the Department of Banking or an applicable federal bank regulatory agency, and **[**(C)**]** (iii) has established a program to comply with all applicable requirements established by the Banking Commissioner or the applicable federal bank regulatory agency concerning personal data; or **[**(12)**]** (L) agent, broker-dealer, investment adviser or investment adviser agent, as such terms are defined in section 36b-3, who is regulated by the Department of Banking or the Securities and Exchange Commission.

(2) The provisions of subdivision (1) of this subsection shall not be construed to excuse a controller from performing the controller's duties in response to the exercise of a consumer's rights afforded under subdivision (6) of subsection (a) of section 42-518, as amended by this act, insofar as such controller is processing the consumer's personal data by automated means for purposes of profiling in furtherance of a solely automated decision that results in the provision or denial by the controller to the consumer of any employment opportunity.

Sec. 14. Subsection (a) of section 42-518 of the 2026 supplement to the general statutes, as amended by section 8 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) A consumer shall have the right to: (1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, including, but not limited to, any inferences about the consumer derived from such personal data and whether a controller or processor is processing a consumer's personal data for the purposes of profiling to make a decision that produces any legal or similarly significant effect concerning a consumer, unless such confirmation or access would require the controller to reveal a trade secret or the controller is prohibited from disclosing such personal data under subsection (e) of this section; (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data; (3) delete personal data provided by, or obtained about, the consumer; (4) obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret; (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subdivision (2) of subsection (a) of section 42-520, as amended by this act, or (C) profiling in furtherance of any automated decision that produces any legal or similarly significant effect concerning the consumer; (6) if the consumer's personal data were processed for the purposes of profiling in furtherance of any automated decision that produced any legal or similarly significant effect concerning the consumer, and if feasible, (A) question the result of such profiling, (B) be informed of the reason that such profiling resulted in such decision, (C) review the consumer's personal data that were processed for the purposes of such profiling, **[**and**]** (D) if the profiling decision concerned housing, taking into account the nature of the

personal data and the purposes for which such personal data were processed, [allow the consumer to] correct any incorrect personal data that were processed for the purposes of such profiling and have the profiling decision reevaluated based on the corrected personal data, and (E) if the profiling decision concerned denial of an employment opportunity, taking into account the nature of the personal data and the purposes for which such personal data were processed, be informed whether any personal data processed for the purposes of such profiling were submitted by a third party, correct any incorrect personal data submitted by a third party that were processed for purposes of such profiling and have the profiling decision reevaluated based on the corrected personal data; and (7) obtain from the controller a list of the third parties to which such controller has sold the consumer's personal data or, if such controller does not maintain a list of the third parties to which such controller has sold the consumer's personal data, a list of all third parties to which such controller has sold personal data, provided the controller shall not be required to reveal any trade secret.

Sec. 15. Subsection (a) of section 42-520 of the 2026 supplement to the general statutes, as amended by section 9 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) (1) A controller shall: (A) Limit the collection of personal data to what is reasonably necessary and proportionate in relation to the purposes for which such data are processed, as disclosed to the consumer; (B) unless the controller obtains the consumer's consent, not process the consumer's personal data for any [material] new purpose that is neither reasonably necessary to, nor compatible with, the purposes that were disclosed to the consumer, pursuant to subparagraph (A) of this subdivision, taking into account (i) the consumer's reasonable expectation regarding such personal data at the time such personal data were collected based on the purposes that were disclosed to the consumer pursuant to subparagraph (A) of this subdivision, (ii) the relationship that such new purpose bears to the purposes that were disclosed to the consumer pursuant to

subparagraph (A) of this subdivision, (iii) the impact that processing such personal data for such new purpose might have on the consumer, (iv) the relationship between the consumer and the controller and the context in which the personal data were collected, and (v) the existence of additional safeguards, including, but not limited to, encryption or pseudonymization, in processing such personal data for such new purpose; (C) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue; (D) not process sensitive data concerning a consumer unless such processing is reasonably necessary in relation to the purposes for which such sensitive data are processed and without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a consumer who the controller has actual knowledge, or wilfully disregards, is a child, without processing such data in accordance with COPPA; (E) not process personal data in violation of any law of this state that prohibits unlawful discrimination against consumers, and any evidence, or lack of evidence, concerning proactive anti-bias testing or any similar proactive effort to avoid processing such data in violation of such law, including, but not limited to, any evidence or lack of evidence concerning the quality, efficacy, recency and scope of any such testing or effort, the results of such testing or effort and the response to the results of such testing or effort, shall be relevant to any claim available for a violation of such law and any defense available thereto; (F) not process personal data in violation of any federal law that prohibits unlawful discrimination against consumers; (G) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; (H) not sell the sensitive data of a consumer without the consumer's consent; and (I) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data, under circumstances where a controller

has actual knowledge, or wilfully disregards, that the consumer is at least thirteen years of age but younger than eighteen years of age. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 42-515 to 42-525, inclusive, as amended by this act, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

(2) Nothing in subdivision (1) of this subsection shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

(3) No controller shall sell, share or transfer, or allow any other person to access, precise geolocation data.

Sec. 16. Subsection (a) of section 42-521 of the 2026 supplement to the general statutes, as amended by section 10 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) (1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 42-515 to 42-525, inclusive, as amended by this act. Such assistance shall include: **[**(1)**]** (A) Taking into account the nature of processing and insofar as is possible, to fulfill the controller's obligation to respond to consumers' requests to exercise their rights under section 42-518, as amended by this act; **[**(2)**]** (B) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in section 36a-701b, of the system of the processor, in order to meet the controller's obligations; and

[(3)**]** (C) providing necessary information to enable the controller to conduct and document data protection assessments and impact assessments.

(2) No processor shall sell, share or transfer, or allow any other person to access, precise geolocation data.

Sec. 17. Subsection (a) of section 42-524 of the 2026 supplement to the general statutes, as amended by section 12 of public act 25-113, is repealed and the following is substituted in lieu thereof (*Effective October 1, 2026*):

(a) (1) Nothing in sections 42-515 to 42-526, inclusive, as amended by this act, shall be construed to restrict a controller's, processor's or consumer health data controller's ability to: **[**(1)**]** (A) Comply with federal, state or municipal ordinances or regulations; **[**(2)**]** (B) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities; **[**(3)**]** (C) cooperate with law enforcement agencies concerning conduct or activity that the controller, processor or consumer health data controller reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations; **[**(4)**]** (D) investigate, establish, exercise, prepare for or defend legal claims; **[**(5)**]** (E) provide a product or service specifically requested by a consumer; **[**(6)**]** (F) perform **[**under**]** pursuant to a contract to which a consumer is a party, including fulfilling the terms of a written warranty; **[**(7)**]** (G) take steps at the request of a consumer prior to entering into a contract; **[**(8)**]** (H) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis; **[**(9)**]** (I) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action; **[**(10)**]** (J) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other

applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, **[**(A)**]** (i) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller or consumer health data controller, **[**(B)**]** (ii) the expected benefits of the research outweigh the privacy risks, and **[**(C)**]** (iii) whether the controller or consumer health data controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; **[**(11)**]** (K) assist another controller, processor, consumer health data controller or third party with any of the obligations under sections 42-515 to 42-526, inclusive, as amended by this act; or **[**(12)**]** (L) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is **[**(A)**]** (i) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data are being processed, and **[**(B)**]** (ii) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(2) (A) Notwithstanding the provisions of subparagraph (I) of subdivision (1) of this subsection, no controller, processor or consumer health data controller shall use any facial recognition technology to prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action, unless: (i) Such facial recognition technology is used exclusively by such controller, processor or consumer health data controller to match still images or video to a database maintained exclusively by such controller, processor or consumer health data controller; and (ii) clearly legible signage is posted at each entrance to the premises where the facial recognition technology described in subparagraph (A)(i) of this subdivision is in use, other than an entrance to an area where access is restricted to authorized employees, (I) alerting consumers entering such premises that facial recognition technology is in use at such premises,

and (II) that includes a conspicuous hyperlink or quick response code that directs consumers to the privacy policy maintained by such controller, processor or consumer health data controller.

(B) Each privacy policy maintained pursuant to subparagraph (A)(ii)(II) of this subdivision shall require the controller, processor or consumer health data controller to: (i) Enable a consumer to (I) readily determine whether the consumer is included in the database described in subparagraph (A)(i) of this subdivision, and (II) if the consumer is included in such database, submit to such controller, processor or consumer health data controller a written request that such consumer be removed from such database; and (ii) not later than fifteen days after such controller, processor or consumer health data controller receives a written request submitted under subparagraph (B)(i)(II) of this subdivision, (I) either grant or deny such request, and (II) send a written notice to the consumer who submitted such request disclosing such controller's, processor's or consumer health data controller's decision, the reasons therefor and, if such controller, processor or consumer health controller denied such request, contact information for the office of the Attorney General.

Sec. 18. (NEW) (*Effective October 1, 2026*) (a) As used in this section:

(1) "Automated license plate reader" means a mobile or fixed electronic device that is capable of recording data on, or taking a photograph or video of, a vehicle or a vehicle's license plate;

(2) "Automated license plate reader information" means information that is (A) gathered by an automated license plate reader, or (B) created through an analysis of the information gathered by an automated license plate reader;

(3) "Automated license plate reader user" means a person who (A) owns or operates an automated license plate reader, or (B) has access to the automated license plate reader information gathered by the automated license plate reader;

(4) "Exigent circumstances" (A) means circumstances that were unforeseeable and pose an imminent threat to public health or safety, (B) includes, but is not limited to, circumstances that would cause a reasonable person to believe that access to automated license plate reader information is necessary to prevent physical harm to an individual, the destruction of evidence or the escape of a suspect, and (C) does not include investigating any suspected immigration violation or otherwise assisting in any immigration enforcement activity;

(5) "Gender-affirming health care services" has the same meaning as provided in section 52-571m of the general statutes;

(6) "Law enforcement agency" has the same meaning as provided in section 54-240 of the general statutes;

(7) "Person" means an individual, association, corporation, limited liability company, partnership, trust or other legal entity;

(8) "Protected health care activity" means (A) seeking, providing or receiving reproductive health care services or gender-affirming health care services, and (B) assisting any other individual who is seeking, providing or receiving reproductive health care services or gender-affirming health care services, including, but not limited to, by providing information, transportation, lodging or material support to such other individual; and

(9) "Reproductive health care services" has the same meaning as provided in section 52-571m of the general statutes.

(b) On and after October 1, 2026, the Department of Transportation, the Department of Motor Vehicles or a law enforcement agency shall not enter into or renew any contract with an automated license plate reader user, unless such contract provides that the automated license plate reader user shall not engage in any of the following activities with respect to any automated license plate reader information gathered in this state:

(1) Sell such automated license plate reader information;

(2) Share or transfer such automated license plate reader information to any person other than the Department of Transportation, the Department of Motor Vehicles or a law enforcement agency;

(3) Allow any person other than the Department of Transportation, the Department of Motor Vehicles or a law enforcement agency to access such automated license plate reader information, unless the automated license plate reader user is required to allow such person to access such automated license plate reader information (A) pursuant to a signed judicial warrant or valid court order issued by a court of competent jurisdiction, or (B) due to the existence of exigent circumstances; or

(4) Share or transfer such automated license plate reader information, or allow access to such automated license plate reader information, if the automated license plate reader user reasonably believes that such automated license plate reader information may be used for purposes of (A) investigating any suspected immigration violation or otherwise assisting in any immigration enforcement activity, (B) investigating any suspected, or prosecuting any alleged, activity, including, but not limited to, any protected health care activity, that is legal in this state, or (C) any effort to identify, or impose any civil or criminal liability on, any person based solely on such person's participation in any activity that is protected by the United States Constitution or the Constitution of the state of Connecticut, including, but not limited to, any exercise of such person's right to freedom of speech, to peaceably assemble or to petition the government for a redress of grievances, except as otherwise provided by applicable state or federal law.

(c) Automated license plate reader information is confidential and shall not be deemed a public record for the purposes of the Freedom of Information Act, as defined in section 1-200 of the general statutes.

(d) The Attorney General may institute proceedings to enforce the provisions of subsections (b) and (c) of this section. In any proceedings instituted under this subsection, the court may grant appropriate relief, including, but not limited to, preliminary, temporary or permanent injunctive relief.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2026*	New section
Sec. 2	*October 1, 2026*	New section
Sec. 3	*October 1, 2026*	New section
Sec. 4	*October 1, 2026*	New section
Sec. 5	*October 1, 2026*	New section
Sec. 6	*October 1, 2026*	New section
Sec. 7	*October 1, 2026*	New section
Sec. 8	*October 1, 2026*	New section
Sec. 9	*October 1, 2026*	New section
Sec. 10	*October 1, 2026*	New section
Sec. 11	*October 1, 2026*	New section
Sec. 12	*October 1, 2026*	42-515
Sec. 13	*October 1, 2026*	42-517(a)
Sec. 14	*October 1, 2026*	42-518(a)
Sec. 15	*October 1, 2026*	42-520(a)
Sec. 16	*October 1, 2026*	42-521(a)
Sec. 17	*October 1, 2026*	42-524(a)
Sec. 18	*October 1, 2026*	New section

Statement of Legislative Commissioners:

In Section 2(c)(5), "shall take" was changed to "will take" for clarity; in Section 2(c)(7), "if such application is" was changed to "for" for internal consistency; in Sections 5(b), 5(c)(1), 5(c)(4) and 18(b), "Beginning on" was changed to "On and after" for consistency with standard drafting conventions; in Section 9, "any provision of" was added for consistency with standard drafting conventions; in Section 14(a)(6)(D), "allow the consumer to" was bracketed for internal consistency; and in Section 14(a)(6)(E), two instances of "allow the consumer to" were deleted for internal consistency.

GL *Joint Favorable Subst.*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact:

Agency Affected	Fund-Effect	FY 27 $	FY 28 $
Consumer Protection, Dept.	GF - Cost	773,523	355,830
State Comptroller - Fringe Benefits[1]	GF - Cost	109,197	145,596
Resources of the General Fund	GF - Potential Revenue Gain	See Below	See Below

Note: GF=General Fund

Municipal Impact: None

Explanation

The bill requires the Department of Consumer Protection (DCP) to register and regulate data brokers, establish and maintain an accessible deletion mechanism program, and enforce various civil penalties/fines and an unfair trade practice violation for certain algorithmic pricing violations resulting in the following costs:

- DCP does not have the resources or expertise to develop the deletion mechanism program and will need to hire a consultant to create the program for a cost of approximately $500,000 in FY 27.

- To meet the requirements of the bill DCP will need to hire four new positions[2] for a salary and other expenses cost of $273,523

[1]The fringe benefit costs for most state employees are budgeted centrally in accounts administered by the Comptroller. The estimated active employee fringe benefit cost associated with most personnel changes is 41.82% of payroll in FY 27.
[2]The positions include a legal program manager, staff attorney, license and application specialist, and inspector.

in FY 27[3] and $355,830 in FY 28, along with associated fringe benefit costs of $109,197 in FY 27 and $145,596 in FY 28.

The bill also creates various civil penalties, fees, and fines which result in a potential revenue gain to the state to the extent fees are paid or violations occur, described below:

- Requires data brokers to be licensed by DCP and pay an initial registration and subsequent annual renewal fees of $600.
- Allows DCP to charge an unspecified fee amount for each registered data broker that accesses the deletion mechanism program.
- Allows DCP to impose a civil penalty of up to $5,000 per day for any violation of sections 2 to 7.
- Requires car manufacturers to put a tariff cost estimate on new cars and allows fines of up to $1,000 to be issued for any violations.

The bill also makes various changes concerning consumer privacy and protection resulting in no fiscal impact to the state.

The Out Years

The annualized ongoing fiscal impact identified above would continue into the future subject to employee wage increases, the number of licenses applied for, the number of violations, and inflation.

[3]Costs in FY 27 reflect nine months of expenditures due to the bill's 10/1/26 effective date.

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)