Senate

General Assembly

File No. 609

January Session, 2025

Substitute Senate Bill No. 1356

Senate, April 9, 2025

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 DATA PRIVACY, ONLINE MONITORING, SOCIAL MEDIA, DATA BROKERS AND CONNECTED VEHICLE SERVICES.

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

Section 1. Section 42-515 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

As used in this section and sections 42-516 to 42-526, inclusive, as amended by this act, 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**]** can be associated with 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 **[**is**]** 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 or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit 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 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, **[**or**]** 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) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

(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) "Gender-affirming health care services" has the same meaning as provided in section 52-571n.

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

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

(22) "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) "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) "Neural data" means any information that is generated by measuring the activity of an individual's central or peripheral nervous system.

[(24)**]** (25) "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.

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

[(26)**]** (27) "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.

[(27)**]** (28) "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.

[(28)**]** (29) "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.

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

[(30)**]** (31) "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.

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

[(32)**]** (33) "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 **[**is**]** are not attributed to an identified or identifiable individual.

[(33)**]** (34) "Publicly available information" means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, **[**and**]** or (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public. "Publicly available information" does not include any (i) information that is collated and combined to create a consumer profile that is made available to a user of a publicly available Internet web site either in exchange for payment or free of charge, (ii) information that is made available for sale, or (iii) inference that is generated from the information described in subparagraph (B)(i) or (B)(ii) of this subdivision.

[(34)**]** (35) "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.

[(35)**]** (36) "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.

[(36)**]** (37) "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.

[(37)**]** (38) "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.

[(38)**]** (39) "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**[**, **[**or**]** 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) **[**the

processing of**]** genetic or biometric data **[**for the purpose of uniquely identifying an individual**]** or information derived therefrom, (D) personal data collected from **[**a known**]** an individual the controller has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, is a child, (E) data concerning an individual's status as a victim of crime, as defined in section 1-1k, **[**or**]** (F) precise geolocation data, (G) neural data, (H) financial information that reveals 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) 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.

[(39)**]** (40) "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.

[(40)**]** (41) "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.

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

Sec. 2. Section 42-516 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

The provisions of sections 42-515 to 42-525, inclusive, as amended by this act, apply to persons that: [conduct] (1) Conduct business in this state, or [persons that] produce products or services that are targeted to residents of this state, and [that] during the preceding calendar year [: (1) Controlled] (A) controlled or processed the personal data of not [less] fewer than [one hundred thousand] thirty-five thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, [;] or [(2)] (B) controlled or processed the personal data of not [less] fewer than [twenty-five thousand] ten thousand consumers and derived more than [twenty-five] twenty per cent of their gross revenue from the sale of personal data; (2) control or process consumers' sensitive data; or (3) offer consumers' personal data for sale in trade or commerce.

Sec. 3. Subsections (a) and (b) of section 42-517 of the general statutes are repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(a) The provisions of sections 42-515 to 42-525, inclusive, as amended by this act, do not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) person who has entered into a contract with any body, authority, board, bureau, commission, district or agency described in 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) [nonprofit organization; (4)] institution of higher education; [(5)] (4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; [(6) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; (7) covered entity or business associate, as defined in 45 CFR 160.103; (8)] (5) tribal nation government organization; or [(9)] (6) 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.

(b) The following information and data [is] are exempt from the provisions of sections 42-515 to 42-526, inclusive, as amended by this act: (1) Protected health information under HIPAA; (2) patient-identifying information for purposes of 42 USC 290dd-2; (3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work product for purposes of section 19a-127o and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; (9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (10) information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities; (11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized

under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time; (15) data processed or maintained (A) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor, consumer health data controller or third party, to the extent that the data **[**is**]** are collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 42-515 to 42-526, inclusive, as amended by this act, used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; **[**and**]** (16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in 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; and (17) data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., as amended from time to time.

Sec. 4. Subsections (a) and (b) of section 42-518 of the general statutes are repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(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, unless such confirmation or access would require the controller to reveal a trade secret; (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; **[**and**]** (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 subsection (b) of section 42-520, or (C) profiling in furtherance of **[**solely**]** automated decisions that produce legal or similarly significant effects concerning the consumer; and (6) obtain from the controller (A) a list of the third parties to which such controller has sold the consumer's personal data, or (B) 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.

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 42-519 to exercise the rights of such consumer to opt out of the processing of such consumer's personal data for purposes of subdivision (5) of subsection (a) of this section on behalf of the consumer. In the case of processing personal data of a **[**known**]** consumer who the controller has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, is a child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

Sec. 5. Subsection (a) of section 42-520 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(a) A controller shall: (1) Limit the collection of personal data to what is [adequate, relevant and] reasonably necessary [in relation to the purposes for which such data is processed, as disclosed to] and proportionate to provide or maintain a product or service specifically requested by the consumer; (2) [except as otherwise provided in sections 42-515 to 42-525, inclusive,] not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data [is] are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent; (3) 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; (4) not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a [known] consumer who the controller has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, is a child, without processing such data in accordance with COPPA; (5) not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers; (6) 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; (7) not sell the sensitive data of a consumer without the consumer's consent; and [(7)] (8) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, or [wilfully disregards] knowledge fairly implied on the basis of objective circumstances, that the consumer is at least thirteen years of age but younger than sixteen 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.

Sec. 6. Subsections (a) to (d), inclusive, of section 42-524 of the general statutes are repealed and the following are substituted in lieu thereof (*Effective October 1, 2025*):

(a) 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) Comply with federal, state or municipal ordinances or regulations; (2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities; (3) 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) investigate, establish, exercise, prepare for or defend legal claims; (5) provide a product or service specifically requested by a consumer; (6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty; (7) take steps at the request of a consumer prior to entering into a contract; (8) 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) 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) 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) 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) the expected benefits

of the research outweigh the privacy risks, and (C) 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) 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) 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) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data **[**is**]** are being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(b) The obligations imposed on controllers, processors or consumer health data controllers under sections 42-515 to 42-526, inclusive, as amended by this act, shall not restrict a controller's, processor's or consumer health data controller's ability to collect, use or retain data for internal use to: (1) Conduct internal research to develop, improve or repair products, services or technology; (2) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform solely internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or consumer health data controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers, processors or consumer health data controllers under sections 42-515 to 42-526, inclusive, as amended by this act, shall not apply where compliance by the controller, processor or consumer health data controller with said sections would violate an evidentiary privilege under the laws of this state. Nothing in sections 42-515 to 42-526, inclusive, as amended by this act, shall be construed to prevent a controller, processor or consumer health data

controller from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(d) A controller, processor or consumer health data controller that discloses personal data to a processor or third-party controller in accordance with sections 42-515 to 42-526, inclusive, as amended by this act, shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller, processor or consumer health data controller disclosed such personal data, the disclosing controller, processor or consumer health data controller did not have actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller, processor or consumer health data controller in compliance with sections 42-515 to 42-526, inclusive, as amended by this act, is likewise not in violation of said sections for the transgressions of the controller, processor or consumer health data controller from which such third-party controller or processor receives such personal data.

Sec. 7. Subsections (a) and (b) of section 42-528 of the general statutes are repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(a) For the purposes of this section:

(1) "Authenticate" means to use reasonable means and make a commercially reasonable effort to determine whether a request to exercise any right afforded under subsection (b) of this section has been submitted by, or on behalf of, the minor who is entitled to exercise such right;

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

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

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

(5) "Social media platform" (A) means a public or semi-public Internet-based service or application that (i) is used by a consumer in this state, (ii) is primarily intended to connect and allow users to socially interact within such service or application, and (iii) enables a user to **[**(I)**]** construct a public or semi-public profile for the purposes of signing into and using such service or application, **[**(II) populate a public list of other users with whom the user shares a social connection within such service or application, and (III) create or post content that is viewable by other users, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users,**]** and (B) does not include a public or semi-public Internet-based service or application that (i) exclusively provides electronic mail or direct messaging services, (ii) primarily consists of news, sports, entertainment, interactive video games, electronic commerce or content that is preselected by the provider or for which any chat, comments or interactive functionality is incidental to, directly related to, or dependent on the provision of such content, or (iii) is used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program; and

(6) "Unpublish" means to remove a social media platform account from public visibility.

(b) (1) Not later than fifteen business days after a social media platform receives a request from a minor or, if the minor is younger than sixteen years of age, from such minor's parent or legal guardian to unpublish such minor's social media platform account, the social media platform shall unpublish such minor's social media platform account.

(2) Not later than forty-five business days after a social media

platform receives a request from a minor or, if the minor is younger than sixteen years of age, from such minor's parent or legal guardian to delete such minor's social media platform account, the social media platform shall delete such minor's social media platform account and cease processing such minor's personal data except where the preservation of such minor's social media platform account or personal data is otherwise permitted or required by applicable law, including, but not limited to, sections 42-515 to 42-525, inclusive, as amended by this act. A social media platform may extend such forty-five business day period by an additional forty-five business days if such extension is reasonably necessary considering the complexity and number of the consumer's requests, provided the social media platform informs the minor or, if the minor is younger than sixteen years of age, such minor's parent or legal guardian within the initial forty-five business day response period of such extension and the reason for such extension.

(3) A social media platform shall establish, and shall describe in a privacy notice, one or more secure and reliable means for submitting a request pursuant to this subsection. A social media platform that provides a mechanism for a minor or, if the minor is younger than sixteen years of age, the minor's parent or legal guardian to initiate a process to delete or unpublish such minor's social media platform account shall be deemed to be in compliance with the provisions of this subsection.

(4) No social media platform shall require a minor's parent or legal guardian to create a social media platform account to submit a request pursuant to this subsection. A social media platform may require a minor's parent or legal guardian to use an existing social media platform account to submit such a request, provided such parent or legal guardian has access to the existing social media platform account.

Sec. 8. Section 42-529a of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(a) Each controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or **[**wilfully

disregards**]** knowledge fairly implied on the basis of objective circumstances, are minors shall use reasonable care to avoid any heightened risk of harm to minors caused by such online service, product or feature. **[**In any enforcement action brought by the Attorney General pursuant to section 42-529e, there shall be a rebuttable presumption that a controller used reasonable care as required under this section if the controller complied with the provisions of section 42-529b concerning data protection assessments.**]**

(b) (1) **[**Subject to the consent requirement established in subdivision (3) of this subsection, no**]** No controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or **[**wilfully disregards**]** knowledge fairly implied on the basis of objective circumstances, are minors shall: (A) Process any minor's personal data (i) for the purposes of (I) targeted advertising, (II) any sale of personal data, or (III) profiling in furtherance of any **[**fully**]** automated decision made by such controller that produces any legal or similarly significant effect concerning the provision or denial by such controller of any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care services or access to essential goods or services, (ii) unless such processing is reasonably necessary to provide such online service, product or feature, (iii) for any processing purpose (I) other than the processing purpose that the controller disclosed at the time such controller collected such personal data, or (II) that is reasonably necessary for, and compatible with, the processing purpose described in subparagraph (A)(iii)(I) of this subdivision, or (iv) for longer than is reasonably necessary to provide such online service, product or feature; or (B) use any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature. The provisions of this subdivision shall not apply to any service or application that is used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program.

(2) **[**Subject to the consent requirement established in subdivision (3)

of this subsection, no**]** No controller that offers an online service, product or feature to consumers whom such controller has actual knowledge, or **[**wilfully disregards**]** knowledge fairly implied on the basis of objective circumstances, are minors shall collect a minor's precise geolocation data unless: (A) Such precise geolocation data **[**is reasonably**]** are strictly necessary for the controller to provide such online service, product or feature and, if such data **[**is**]** are necessary to provide such online service, product or feature, such controller may only collect such data for the time necessary to provide such online service, product or feature; and (B) the controller provides to the minor a signal indicating that such controller is collecting such precise geolocation data, which signal shall be available to such minor for the entire duration of such collection.

[(3) No controller shall engage in the activities described in subdivisions (1) and (2) of this subsection unless the controller obtains the minor's consent or, if the minor is younger than thirteen years of age, the consent of such minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in 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, shall be deemed to have satisfied any requirement to obtain parental consent under this subdivision.**]**

(c) (1) No controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or **[**wilfully disregards**]** knowledge fairly implied on the basis of objective circumstances, are minors shall: (A) Provide any consent mechanism that is designed to substantially subvert or impair, or is manipulated with the effect of substantially subverting or impairing, user autonomy, decision-making or choice; or (B) except as provided in subdivision (2) of this subsection, offer any direct messaging apparatus for use by minors without providing readily accessible and easy-to-use safeguards to limit the ability of adults to send unsolicited communications to

minors with whom they are not connected.

(2) The provisions of subparagraph (B) of subdivision (1) of this subsection shall not apply to services where the predominant or exclusive function is: (A) Electronic mail; or (B) direct messaging consisting of text, photos or videos that are sent between devices by electronic means, where messages are (i) shared between the sender and the recipient, (ii) only visible to the sender and the recipient, and (iii) not posted publicly.

Sec. 9. Subsection (a) of section 42-529b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(a) Each controller that **[**, on or after October 1, 2024,**]** offers any online service, product or feature to consumers whom such controller has actual knowledge, or **[**wilfully disregards**]** knowledge fairly implied on the basis of objective circumstances, are minors shall conduct a data protection assessment for such online service, product or feature: (1) In a manner that is consistent with the requirements established in section 42-522; and (2) that addresses (A) the purpose of such online service, product or feature, (B) the categories of minors' personal data that such online service, product or feature processes, (C) the purposes for which such controller processes minors' personal data with respect to such online service, product or feature, and (D) any heightened risk of harm to minors that is a reasonably foreseeable result of offering such online service, product or feature to minors.

Sec. 10. Subsection (d) of section 42-529d of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(d) No obligation imposed on a controller or processor under any provision of sections 42-529 to 42-529c, inclusive, or section 42-529e shall be construed to restrict a controller's or processor's ability to collect, use or retain data for internal use to: (1) Conduct internal research to develop, improve or repair products, services or technology; (2)

effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform solely internal operations that are (A) reasonably aligned with the expectations of a minor or reasonably anticipated based on the minor's existing relationship with the controller or processor, or (B) otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a minor.

Sec. 11. (NEW) (*Effective October 1, 2025*) (a) As used in this section:

(1) "Brokered personal data" means any personal data that are categorized or organized for the purpose of enabling a data broker to sell or license such personal data to another person;

(2) "Business" (A) means (i) a person who regularly engages in commercial activities for the purpose of generating income, (ii) a bank, Connecticut credit union, federal credit union, out-of-state bank, out-of-state trust company or out-of-state credit union, as said terms are defined in section 36a-2 of the general statutes, and (iii) any other person that controls, is controlled by or is under common control with a 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;

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

(4) "Data broker" means any business or, if such business is an entity, any portion of such business that sells or licenses brokered personal data to another person;

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

(6) "License" (A) means to grant access to, or distribute, personal data in exchange for consideration, and (B) does not include any use of 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;

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

(8) "Personal data" (A) means any data concerning a consumer that, either alone or in combination with any other data that are sold or licensed by a data broker to another person, can reasonably be associated with the consumer, and (B) includes, but is not limited to, (i) a consumer's name or the name of any member of the consumer's immediate family or household, (ii) a consumer's address or the address of any member of the consumer's immediate family or household, (iii) a consumer's birth date or place of birth, (iv) the maiden name of a consumer's mother, (v) biometric data, as defined in section 42-515 of the general statutes, as amended by this act, concerning a consumer, and (vi) a consumer's Social Security number or any other government-issued identification number issued to the consumer.

(b) (1) Except as provided in subdivision (4) of this subsection and subsection (d) of this section, no data broker shall sell or license brokered personal data in this state unless the data broker is actively registered with the Department of Consumer Protection in accordance with the provisions of this subsection. A data broker who desires to sell or license brokered personal data in this state shall submit an application to the department in a form and manner prescribed by the Commissioner of Consumer Protection. Each application for registration as a data broker shall be accompanied by a registration fee in the amount of six hundred dollars. Each registration issued pursuant to this subsection shall expire on December thirty-first of the year in which such registration was issued and may be renewed for successive one-year terms upon application made in the manner set forth in this subsection and payment of a registration renewal fee in the amount of six hundred dollars.

(2) Except as provided in subdivision (4) of this subsection, each application submitted to the department pursuant to subdivision (1) of this subsection shall include:

(A) The applicant's name, mailing address, electronic mail address

and telephone number;

(B) The address of the applicant's primary Internet web site; and

(C) A statement by the applicant disclosing the measures the applicant shall take to ensure that no personal data is sold or licensed in violation of the provisions of sections 42-515 to 42-525, inclusive, of the general statutes, as amended by this act.

(3) The department shall make all information that an applicant submits to the department pursuant to subdivision (2) of this subsection publicly available on the department's Internet web site.

(4) The department 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.

(c) No data broker shall sell or license any personal data in violation of the provisions of sections 42-515 to 42-525, inclusive, of the general statutes, as amended by this act. Each data broker shall implement measures to ensure that the data broker does not sell or license any personal data in violation of the provisions of sections 42-515 to 42-525, inclusive, of the general statutes, as amended by this act.

(d) (1) The provisions of this section shall not apply to: (A) A consumer reporting agency, as defined in 15 USC 1681a(f), as amended from time to time, a person that 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; (B) a financial institution, an affiliate or a nonaffiliated third party, as said 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 regulations may be amended from time to time; (C) a business that collects information concerning a consumer if the consumer (i) is a customer, subscriber or user of goods or services sold or offered by the business, (ii) is in a contractual relationship with the business, (iii) is an investor in the business, (iv) is a donor to the business, or (v) otherwise maintains a relationship with the business that is similar to the relationships described in subparagraphs (C)(i) to (C)(iv), inclusive, of this subdivision; or (D) a business that performs services for, or acts as an agent or on behalf of, a business described in subparagraph (C) of this subdivision.

(2) No provision of this section 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: (A) Publicly available information (i) concerning a consumer's business or profession, or (ii) sold or licensed as part of a service that provides alerts for health or safety purposes; (B) information that is lawfully available from any federal, state or local government record; (C) providing digital access to any (i) journal, book, periodical, newspaper, magazine or news media, or (ii) educational, academic or instructional work; (D) developing or maintaining an electronic commerce service or software; (E) providing directory assistance or directory information services as, or on behalf of, a telecommunications carrier; or (F) 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.

(e) 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 this section.

(f) 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 hundred dollars per day for each violation of subsections (b) to (d), inclusive, of this section. The sum of civil penalties imposed on a data broker pursuant to this subsection shall not exceed ten thousand dollars during any calendar year.

Sec. 12. (NEW) (*Effective January 1, 2026*) (a) As used in this section:

(1) "Abuser" means an individual who (A) is identified by a survivor pursuant to subsection (b) of this section, and (B) has committed, or allegedly committed, a covered act against the survivor making the connected vehicle services request;

(2) "Account holder" means an individual who is (A) a party to a contract with a covered provider that involves a connected vehicle service, or (B) a subscriber, customer or registered user of a connected vehicle service;

(3) "Connected vehicle service" means any capability provided by or on behalf of a motor vehicle manufacturer that enables a person to remotely obtain data from, or send commands to, a covered vehicle, including, but not limited to, any such capability provided by way of a software application that is designed to be operated on a mobile device;

(4) "Connected vehicle service request" means a request by a survivor to terminate or disable an abuser's access to a connected vehicle service;

(5) "Covered act" means conduct that constitutes (A) a crime described in Section 40002(a) of the Violence Against Women Act of 1994, 34 USC 12291(a), as amended from time to time, (B) an act or practice described in 22 USC 7102(11) or (12), as amended from time to time, or (C) a crime, act or practice that is (i) similar to a crime, act or practice described in subparagraph (A) or (B) of this subdivision, and (ii) prohibited under federal, state or tribal law;

(6) "Covered connected vehicle services account" means an account or other means by which a person enrolls in, or obtains access to, a connected vehicle service;

(7) "Covered provider" means a motor vehicle manufacturer, or an entity acting on behalf of a motor vehicle manufacturer, that provides a connected vehicle service;

(8) "Covered vehicle" means a motor vehicle that is (A) the subject of a connected vehicle request, and (B) identified by a survivor pursuant to subsection (b) of this section;

(9) "Emergency situation" means a situation that, if allowed to continue, poses an imminent risk of death or serious bodily harm;

(10) "In-vehicle interface" means a feature or mechanism installed in a motor vehicle that allows an individual within the motor vehicle to terminate or disable connected vehicle services;

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

(12) "Survivor" means an individual (A) who is eighteen years of age or older, and (B) against whom a covered act has been committed or allegedly committed.

(b) A survivor may submit a connected vehicle service request to a covered provider pursuant to this subsection. Each connected vehicle service request submitted pursuant to this subsection shall, at a minimum, include (1) the vehicle identification number of the covered vehicle, (2) the name of the abuser, and (3) (A) proof that the survivor is the sole owner of the covered vehicle, (B) if the survivor is not the sole owner of the covered vehicle, proof that the survivor is legally entitled to exclusive possession of the covered vehicle, which proof may take the form of a court order awarding exclusive possession of the covered vehicle to the survivor, or (C) if the abuser owns the covered vehicle, in whole or in part, a dissolution of marriage decree, restraining order or temporary restraining order (i) naming the abuser, and (ii) (I) granting exclusive possession of the covered vehicle to the survivor, or (II) restricting the abuser's use of a connected vehicle service against the

survivor.

(c) (1) Not later than two business days after a survivor submits a connected vehicle service request to a covered provider pursuant to subsection (b) of this section, the covered provider shall take one or more of the following actions requested by the survivor in the connected vehicle service request, regardless of whether the abuser identified in the connected vehicle service request is an account holder: (A) Terminate or disable the covered connected vehicle services account associated with such abuser; (B) (i) terminate or disable the covered connected vehicle services account associated with the covered vehicle, including, but not limited to, by resetting or deleting any data or wireless connection with respect to the covered vehicle, and (ii) provide instructions to the survivor on how to reestablish a covered connected vehicle services account; (C) (i) terminate or disable covered connected vehicle services for the covered vehicle, including, but not limited to, by resetting or deleting any data or wireless connection with respect to the covered vehicle, and (ii) provide instructions to the survivor on how to reestablish connected vehicle services; or (D) if the motor vehicle has an in-vehicle interface, provide information to the survivor concerning (i) the availability of the in-vehicle interface, and (ii) how to terminate or disable connected vehicle services using the in-vehicle interface.

(2) After the covered provider has taken action pursuant to subdivision (1) of this subsection, the covered provider shall deny any request made by the abuser to obtain any data that (A) were generated by the connected vehicle service after the abuser's access to such connected vehicle service was terminated or disabled in response to the connected vehicle service request, and (B) are maintained by the covered provider.

(3) The covered provider shall not refuse to take action pursuant to subdivision (1) of this subsection on the basis that any requirement, other than a requirement established in subsection (b) of this section, has not been satisfied, including, but not limited to, any requirement that provides for (A) payment of any fee, penalty or other charge, (B)

maintaining or extending the term of the covered connected vehicle services account, (C) obtaining approval from any account holder other than the survivor, or (D) increasing the rate charged for the connected vehicle service.

(4) (A) If the covered provider intends to provide any formal notice to the abuser regarding any action set forth in subdivision (1) of this subsection, the covered provider shall first notify the survivor of the date on which the covered provider intends to provide such notice to the abuser.

(B) The covered provider shall take reasonable steps to ensure that the covered provider only provides formal notice to the abuser, pursuant to subparagraph (A) of this subdivision, (i) at least three days after the covered provider notified the survivor pursuant to subparagraph (A) of this subdivision, and (ii) after the covered provider has terminated or disabled the abuser's access to the connected vehicle service.

(5) (A) The covered provider shall not be required to take any action pursuant to subdivision (1) of this subsection if the covered provider cannot operationally or technically effectuate such action.

(B) If the covered provider cannot operationally or technically effectuate any action as set forth in subparagraph (A) of this subdivision, the covered provider shall promptly notify the survivor who submitted the connected vehicle service request that the covered provider cannot operationally or technically effectuate such action, which notice shall, at a minimum, disclose whether the covered provider's inability to operationally or technically effectuate such action can be remedied and, if so, any steps the survivor can take to assist the covered provider in remedying such inability.

(d) (1) The covered provider and each officer, director, employee, vendor or agent of the covered provider shall treat all information submitted by the survivor under subsection (b) of this section as confidential, and shall securely dispose of such information not later

than ninety days after the survivor submitted such information.

(2) The covered provider shall not disclose any information submitted by the survivor under subsection (b) of this section to a third party unless (A) the covered provider has obtained affirmative consent from the survivor to disclose such information to the third party, or (B) disclosing such information to the third party is necessary to effectuate the connected vehicle service request.

(3) Nothing in subdivision (1) of this subsection shall be construed to prohibit the covered provider from maintaining, for longer than the period specified in subdivision (1) of this subsection, a record that verifies that the survivor fulfilled the conditions of the connected vehicle service request as set forth in subsection (b) of this section, provided such record is limited to what is reasonably necessary and proportionate to verify that the survivor fulfilled such conditions.

(e) The survivor shall take reasonable steps to notify the covered provider of any change in the ownership or possession of the covered vehicle that materially affects the need for the covered provider to take action pursuant to subdivision (1) of subsection (c) of this section.

(f) The requirements established in this section shall not prohibit or prevent a covered provider from terminating or disabling an abuser's access to a connected vehicle service in an emergency situation after receiving a connected vehicle service request.

(g) Each covered provider shall publicly post, on such covered provider's Internet web site, a statement describing how a survivor may submit a connected vehicle service request to such covered provider.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2025*	42-515
Sec. 2	*October 1, 2025*	42-516
Sec. 3	*October 1, 2025*	42-517(a) and (b)
Sec. 4	*October 1, 2025*	42-518(a) and (b)

Sec. 5	*October 1, 2025*	42-520(a)
Sec. 6	*October 1, 2025*	42-524(a) to (d)
Sec. 7	*October 1, 2025*	42-528(a) and (b)
Sec. 8	*October 1, 2025*	42-529a
Sec. 9	*October 1, 2025*	42-529b(a)
Sec. 10	*October 1, 2025*	42-529d(d)
Sec. 11	*October 1, 2025*	New section
Sec. 12	*January 1, 2026*	New section

Statement of Legislative Commissioners:
In Section 11(f), "subsections (b) to (d), inclusive, of" was added before "this section" for consistency with standard drafting conventions; and in Section 12(g), "to such covered provider" was added after "request" for clarity.

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 26 $	FY 27 $
Consumer Protection, Dept.	GF - Cost	154,000	199,000
State Comptroller - Fringe Benefits[1]	GF - Cost	60,535	80,714
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 license and regulate data brokers resulting in a cost and potential revenue gain to the state. To meet the requirements of the bill DCP will have to hire a state program manager and a staff attorney for a cost of $154,000 in FY 26[2] and $199,000 in FY 27, along with associated fringe benefit costs of $60,535 in FY 26 and $80,714 in FY 27. The new employees are required to regulate the market, ensure compliance, conduct hearings, and issue civil penalties for violations.

The bill requires DCP to oversee the registration of data brokers for an annual application and renewal fee of $600 and allows DCP to impose a civil penalty of $500 per day (not to exceed $10,000 per year) for violations resulting in a potential revenue gain to the state to the

[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 40.71% of payroll in FY 26.
[2]FY 26 costs reflect nine months of expenditures due to the bill's 10/2/25 effective date.

extent applications are received and that violations occur.

The bill also changes various data privacy laws 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 the number of applications, number of violations, employee wage increases, and inflation.

OLR Bill Analysis

sSB 1356

AN ACT CONCERNING DATA PRIVACY, ONLINE MONITORING, SOCIAL MEDIA, DATA BROKERS AND CONNECTED VEHICLE SERVICES.

SUMMARY

This bill expands various aspects of the Connecticut Data Privacy Act (CTDPA). Among other things, the bill:

1. expands who is covered under the CTDPA, by lowering the applicability threshold and including those who (a) control or process a consumer's sensitive data or (b) offer a consumer's personal data for sale in trade or commerce;

2. removes current CTDPA exemptions, thus applying its requirements and restrictions to certain additional entities (e.g., nonprofit organizations);

3. expands various aspects of the CTDPA, including what is considered sensitive data and prohibits controllers (entities that determine the purpose and means of processing personal data) from selling a consumer's sensitive data without the consumer's consent;

4. changes the standard for establishing knowledge of a consumer's minor-status as it pertains to certain requirements and restrictions by creating a new "fairly implied knowledge" standard (see below); and

5. prohibits controllers that offer online services, products, or features to minors from performing certain actions (e.g., processing a minor's personal data for targeted advertising and personal data sales) by eliminating the provision that currently

allows them to do so with consent.

Additionally, the bill generally requires a data broker to be actively registered with the Department of Consumer Protection (DCP) before selling or licensing brokered personal data in Connecticut.

It also creates a process by which a survivor of certain crimes (e.g., domestic violence) can submit a request to the motor vehicle manufacturer with a connected vehicle services account to take certain actions to prevent the abuser from remotely obtaining data from, or sending commands to, the survivor's vehicle or one that is under the survivor's exclusive possession or control legally.

Lastly, it makes various minor, technical, and conforming changes.

EFFECTIVE DATE: October 1, 2025, except the motor vehicle data privacy provision is effective January 1, 2026.

§§ 1-9 — CTDPA

Expansion of Applicability

The bill expands the individuals and entities covered by the CTDPA's requirements by lowering certain thresholds and adding additional qualifications.

Under current law, the CTDPA applies to individuals and entities that do business in Connecticut or produce products or services targeting Connecticut residents and, during the preceding calendar year, controlled or processed personal data of at least:

1. 100,000 consumers, excluding personal data controlled or processed solely for completing a payment transaction, or

2. 25,000 consumers and derived more than 25% of their gross revenue from selling personal data.

The bill lowers these thresholds to (1) 35,000 consumers, excluding personal data controlled or processed solely for completing a payment transaction, or (2) 10,000 consumers and derived more than 20% of their

gross revenue from selling personal data.

The bill also extends the CTDPA to cover those that (1) control or process a consumer's sensitive data (see below) or (2) offer a consumer's personal data for sale in trade or commerce.

Sensitive Data

Existing law prohibits controllers from processing sensitive data about a consumer (1) without consent, or (2) if the consumer is known to be a child under age 13, without following the federal Children's Online Privacy Protection Act (COPPA) (15 U.S.C. § 6501 et seq.). Controllers must also conduct and document a data protection assessment for each of their processing activities that presents a heightened risk of harm to consumers, including the processing of sensitive data.

The bill prohibits a controller from selling a consumer's sensitive data without the consumer's consent.

Under current law, "sensitive data" is personal data that includes, among other things, (1) data revealing a mental or physical health condition or diagnosis, (2) processing genetic or biometric data to uniquely identify an individual, and (3) personal data collected from someone known to be a child.

The act expands the "sensitive data" covered by the law by:

1. including data revealing (a) a mental or physical disability or treatment or (b) nonbinary or transgender status;

2. specifying that it includes genetic or biometric data or information derived from the data, rather than only the data processing, to uniquely identify an individual; and

3. including personal data collected from an individual the controller has knowledge, fairly implied on the basis of objective circumstances, is a child, rather than just actual knowledge as required under current law.

The bill also includes the following as sensitive data:

1. neural data (any information generated by measuring the activity of an individual's central or peripheral nervous system);

2. financial information that reveals a consumer's financial account number, financial account log-in information, or credit or debit card numbers that, in combination with any required access or security code, password, or credential, would allow access to a consumer's financial account; or

3. government-issued identification number, including Social Security number, passport number, state identification card number, or driver's license number, that applicable law does not require to be publicly displayed.

Under current law, "biometric data" is data generated by automatic measurements of an individual's biological characteristics that are used to identify a specific individual. The bill expands this to include data that can be associated with a specific individual.

Publicly Available Information

Under current law, "publicly available information" is information that (1) is lawfully available through federal, state, or municipal government records or widely distributed media and (2) a controller has a reasonable basis to believe the consumer has lawfully made available to the general public. Under the bill, either condition is enough for the information to be considered publicly available.

Under existing law, "personal data" does not include publicly available information. Thus, publicly available information is not subject to the CTDPA.

The bill specifies the following are not considered publicly available information:

1. information compiled and combined to create a consumer profile made available to a user of a publicly available Internet website

either for payment or free of charge,

2. information that is made available for sale, or

3. any inference generated from the information described above.

Consumer Health Data

The CTDPA sets standards on accessing and sharing consumer health data and places various specific limitations on consumer health data controllers. The bill expands what is considered "consumer health data" by including personal data that a controller uses to identify a consumer's physical or mental health status. Current law includes personal data used to identify such a condition or diagnosis.

Exemption Removal

The bill removes the following from current law's list of exempted entities, thus subjecting them to CTDPA requirements:

1. nonprofit organizations;

2. financial institutions or data subject to certain provisions of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); and

3. covered entities or business associates, as defined under HIPAA regulations (e.g., health plans, health care clearinghouses, and health care providers).

Consumer Rights

Under current law, a consumer has the right to confirm whether or not a controller is processing the consumer's personal data and access the data. The bill specifies that this includes any inferences about the consumer that is derived from the personal data. As under existing law, this right is available unless the confirmation or access would require the controller to reveal a trade secret.

The bill also expands a consumer's right to opt out of personal data processing when the data is used for profiling to advance any, rather than only, automated decisions that produce legal or similarly

significant effects concerning the consumer.

The bill also gives a consumer the right to obtain from the controller (1) a list of the third parties to whom the controller has sold the consumer's personal data or (2) if the controller does not maintain such a list, a list of all third parties to whom the controller has sold personal data.

Controller Requirement

Under current law, a controller must limit the collection of personal data to what is adequate, relevant, and reasonably necessary for data processing, as disclosed to the consumer. The bill instead requires the collection to be reasonably necessary and proportionate to providing or maintaining a product or service the consumer specifically requests.

§§ 1 & 4-9 — KNOWLEDGE FAIRLY IMPLIED

The bill changes the knowledge element needed for several CTDPA requirements to apply, specifically in instances regarding knowledge of a consumer's minor status. Under current law, actual knowledge is required. The bill expands this to include instances where the knowledge is fairly implied based on objective circumstances. The new fairly implied knowledge standard applies to provisions:

1. allowing a parent or legal guardian to exercise consumer rights on a child's behalf for personal data processing and

2. prohibiting controllers from processing sensitive data concerning a child in accordance with COPPA.

Under the CTDPA, several requirements and prohibitions require actual knowledge or the willful disregard of knowing the consumer is a minor. The bill changes the willfully disregards standard to the knowledge fairly implied standard described above for provisions:

1. prohibiting controllers from processing a consumer's personal data for targeted advertising, or selling the data without the consumer's consent, for consumers ages 13-15;

2. requiring controllers that offer any online service, product, or feature to consumers who are minors to use reasonable care to avoid any heightened risk of harm to them;

3. prohibiting controllers that offer online services, products, or features to consumers who are minors from (a) taking certain actions (e.g., processing a minor's data for certain purposes); (b) collecting precise geolocation data; and (c) providing certain consent mechanisms that are designed to impair user autonomy, among other things; and

4. requiring controllers that offer online services, products, or features to consumers who are minors to conduct a data protection assessment for the online service, product, or feature.

Under current law, controllers, consumer health data controllers, or processors that disclose personal data to a third party under the law's requirements are not responsible for third party violations if at the time of disclosure, the original controllers or processors did not have actual knowledge that the recipient would violate the law. The bill also limits liability in instances when the controllers and processors did not have knowledge fairly implied on the basis of objective circumstances that the recipient would violate the law.

§§ 6 & 10 — INTERNAL OPERATIONS

The CTDPA specifies that the obligations it imposes on controllers, processors, and consumer health data controllers do not restrict their ability to collect, use, or retain data for internal use to, among other things, perform internal operations such as those that are reasonably aligned with the consumer's expectations. The bill narrows the internal operation performances under these provisions to instances where the controllers and processors perform solely internal operations.

§§ 7-10 — MINORS AND ONLINE SERVICES, PRODUCTS, AND FEATURES

Social Media Platform

Under current law, a "social media platform" is a public or semi-

public Internet-based service or application that:

1. is used by a Connecticut consumer;

2. is primarily intended to connect and allow users to socially interact within the service or application; and

3. enables a user to (a) construct a public or semi-public profile for signing into and using the service or application; (b) populate a public list of other users with whom the user shares a social connection within the service or application; and (c) create or post content that is viewable by other users, including on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users.

The bill limits what features platforms must enable users to do to be considered a social media platform. Specifically, it eliminates the requirement that they must also enable users to (1) populate other users' public lists and (2) create or post content that is viewable to others. In doing this, the bill expands what is considered a social media platform under the law.

Prohibition on Requiring Social Media Account for Request

The bill prohibits social media platforms from requiring a minor's parent or legal guardian to create a social media account to submit a request to unpublish the minor's social media platform account. But the platform may require the parent or legal guardian to use an existing account to submit the request, as long as the parent or legal guardian has access to the existing account.

Rebuttable Presumption

In enforcement actions that the attorney general takes, the bill removes current law's rebuttable presumption that the controller used reasonable care as required under the law.

Consent Provision Eliminated

Under current law, controllers that offer online services, products, or

features to minors may perform certain actions if they receive the minor's consent or, if the minor is younger than age 13, that of the minor's parent or legal guardian. The bill prohibits these actions by eliminating the ability for anyone to consent to them.

The following actions are prohibited under current law unless the requisite consent is received, but under the bill no one can consent to them:

1. processing a minor's personal data for targeted advertising and personal data sales, profiling to further certain automated decisions (see below), or collecting the minor's precise geolocation and

2. using a system design feature to significantly increase, sustain, or extend a minor's use of the online service, product, or feature.

Automated Decisions

The bill prohibits controllers that offer any online service, product, or feature to a minor from profiling to advance any automated decisions that produce legal or similarly significant effects concerning the consumer. Current law limits this to apply only when the decision being advance is fully automated.

Precise Geolocation

The bill further limits when a controller that offers an online service, product, or feature to minors may collect a minor's precise geolocation data to circumstances under which it is strictly, rather than reasonably, needed for the controller to provide the online service, product, or feature.

§ 11 — BROKERED PERSONAL DATA

The bill generally requires a data broker to be actively registered with DCP before selling or licensing brokered personal data in Connecticut.

Under the bill, a "data broker" is any business or, if the business is an entity, any portion of the business that sells or licenses brokered

personal data to another person.

A "business" is (1) a person (i.e. individual or entity) that regularly engages in commercial activities to generate income; (2) a bank, Connecticut credit union, federal credit union, out-of-state bank, out-of-state trust company, or out-of-state credit union; and (3) any other person that controls, is controlled by or is under common control with a person described above. A business does not include any state body, authority, board, bureau, commission, district, or agency of the state or its political subdivisions.

"Brokered personal data" is personal data categorized or organized to enable a data broker to sell or license it to another person.

"Personal data" is any consumer-related data that, either alone or in combination with any other data that a data broker sells or licenses to another person, can reasonably be associated with the consumer. It includes the consumer's:

1. name or address, or that of his or her household or immediate family member;
2. birth date or place of birth;
3. mother's maiden name;
4. biometric data as under the CTDPA (see above); and
5. Social Security number or any other government-issued identification number issued to the consumer.

Application

Under the bill, a data broker who wants to sell or license brokered personal data in Connecticut must apply for registration as a data broker to DCP in a form and manner the commissioner prescribes. Each registration application must be accompanied by a $600 registration fee. A registration expires on December 31 of the year in which it was issued and may be annually renewed for a $600 fee under a renewal application

procedure that is the same as the initial application procedure.

Except for registrations that DCP approves or renews based on a data broker complying with an agreement between DCP and the Nationwide Multistate Licensing System, the following must be included in each application:

1. the applicant's name, mailing address, email address, telephone number, and primary Internet website address and

2. a statement by the applicant disclosing the measures he or she must take to ensure that no personal data is sold or licensed in violation of the CTDPA.

DCP must make all the application information described above publicly available on its website.

Data Sale Prohibition

Under the bill, data brokers are prohibited from selling or licensing personal data in violation of the CTDPA and must implement safeguards to prevent these actions.

Exemptions

The bill exempts the following entities from its data broker provisions:

1. consumer reporting agencies, as defined under federal law (15 U.S.C. § 1681 et seq.);

2. financial institutions, affiliates, or nonaffiliated third parties, to the extent that they are involved in activities regulated under Title V of the Gramm-Leach-Bliley Act, (15 U.S.C. § 6801 et seq.);

3. businesses that collect information about consumers who are (a) customers, subscribers, or users of goods or services they sell or offer; (b) in a contractual relationship with them; (c) business investors; (d) business donors; or (e) in any similar relationship with them; or

4. businesses that perform services for, or act as agents or on behalf of, a business described above.

Unregistered Data Broker's Permitted Actions

The bill specifies that it does not prohibit an unregistered data broker from selling or licensing brokered personal data if the sale or license exclusively involves:

1. publicly available information (a) concerning a consumer's business or profession or (b) sold or licensed as part of a service that provides health or safety alerts;

2. lawfully available information from any federal, state, or local government record;

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

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

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

6. a one-time or occasional disposition of business assets as part of a transfer of control over the assets that is not part of the business's ordinary conduct.

Regulations

The bill allows the DCP commissioner to adopt implementing regulations for the bill's data broker provisions.

Penalties

Under the bill, the DCP commissioner, after providing notice and holding a hearing under the Administrative Procedure Act, may impose maximum civil penalties of $500 per day for each data broker violation, up to $10,000 per calendar year.

§ 12 — MOTOR VEHICLE DATA PRIVACY FOR SURVIVORS OF CERTAIN CRIMES

The bill allows survivors of certain crimes (e.g., domestic violence) to submit a connected vehicle service request to a covered provider (i.e. motor vehicle manufacturer, or an entity acting on its behalf, that provides a connected vehicle service) to take certain actions to prevent an abuser (see definition below) from remotely obtaining data from, or sending commands to, a vehicle.

Definitions

Under the bill, a "survivor" is an adult (age 18 or older) against whom a covered act was committed or allegedly committed.

A "covered act" is an action that constitutes:

1. a crime under the federal Violence Against Women Act of 1994, such as domestic violence, dating violence, economic abuse, and stalking (34 U.S.C. § 12291(a));

2. severe forms of trafficking in persons or sex trafficking under federal law (22 U.S.C. § 7102(11) & (12)); or

3. a crime, act, or practice that is (a) similar to those described above and (b) prohibited under federal, state, or tribal law.

A "connected vehicle service request" is a survivor's request to terminate or disable the abuser's access to a connected vehicle service.

An "abuser" is an individual who (1) a survivor identifies in a connected vehicle service request, and (2) has committed, or allegedly committed, a covered act against the survivor who made the service request.

A "connected vehicle service" is any capability a motor vehicle manufacturer provides that allows a person to remotely obtain data from, or send commands to, a covered vehicle, including through a mobile device software application.

A "covered vehicle" is one that is (1) the subject of a connected vehicle request and (2) identified by a survivor under the bill's provisions.

Survivor's Connected Vehicle Service Request

Under the bill, survivors requesting that a connected vehicle service be terminated or disabled must include the vehicle identification number (VIN), the abuser's name, and certain proof of ownership or possession over the vehicle. Proof of ownership or possession must include at least the following, as applicable:

1. proof that the survivor is the vehicle's sole owner;

2. if the survivor is not the sole owner, proof that the survivor is legally entitled to exclusively possess the vehicle, such as a court order awarding exclusive possession of the vehicle to the survivor; or

3. if the abuser owns the vehicle, in whole or in part, a dissolution of marriage decree, restraining order, or temporary restraining order that names the abuser, and (a) gives the survivor exclusive possession of the vehicle or (b) restricts the use of a vehicle service by the abuser against the survivor.

Covered Provider Required Actions

Within two business days after a survivor submits a connected vehicle service request, the covered provider must take one or more of the following actions, whether or not the abuser is an account holder:

1. terminate or disable the covered connected vehicle services account associated with the abuser;

2. terminate or disable the covered connected vehicle services or services account associated with the covered vehicle, including by resetting or deleting its data or wireless connection, and giving the survivor instructions on how to reestablish the services or account; or

3. if the motor vehicle has an in-vehicle interface, informing the

survivor about the interface's availability, and providing information on how to use it to terminate or disable the connected vehicle services.

Denial of Abuser Request

After the covered provider has acted, the provider must deny any request the abuser makes to obtain data (1) generated by the connected vehicle service after the abuser's access to the service was terminated or disabled due to the survivor's request and (2) that the covered provider maintains.

Covered Provider's Requirement to Act

Other than for a service request lacking the required information, the bill prohibits a covered provider from refusing to take the actions listed above based on other requirements not being satisfied, including any requirement for:

1. paying any fee, penalty, or other charge;

2. maintaining or extending the term of the covered connected vehicle services account;

3. obtaining approval from any account holder other than the survivor; or

4. increasing the rate charged for the connected vehicle service.

Notice to Survivor Required Before Notifying Abuser

If the covered provider intends to give the abuser any formal notice about any of the actions above, the provider must first notify the survivor about when it intends to do so.

The bill requires the covered provider to take reasonable steps to ensure that it only gives the abuser formal notice (1) at least three days after the provider notified the survivor and (2) after the provider has terminated or disabled the abuser's access to the connected vehicle service.

When Action is Not Operationally or Technically Feasible

Under the bill, covered providers are not required to take any of the actions above if the provider cannot operationally or technically perform them. If that is the case, the provider must promptly notify the survivor who submitted the request. The notice must at least disclose whether the covered provider's inability to perform the action operationally or technically can be remedied and any steps the survivor can take to assist the provider in doing so.

Confidentially of Request-Related Information

The covered provider and its officers, directors, employees, vendors, or agents must treat all information the survivor submits as confidential and must securely dispose the information within 90 days after the survivor's submission. A covered provider is prohibited from disclosing connected vehicle service request-related information to a third party unless the (1) survivor affirmatively consents or (2) disclosure is necessary to perform the connected vehicle service request.

The bill specifically allows covered providers to maintain certain records for longer than 90 days if the records are reasonably necessary and proportionate to verify that the survivor fulfilled the conditions.

Material Change Notifications

The survivor must take reasonable steps to notify the covered provider about any change in the ownership or possession of the covered vehicle that materially affects the need for the covered provider to take the required actions listed above.

Emergency Situations

Regardless of the requirements above, the bill does not prohibit or prevent a covered provider from terminating or disabling an abuser's access to a connected vehicle service in an emergency situation after receiving a connected vehicle service request.

Website Instructions

The bill requires each covered provider to publicly post on its website

a statement describing how a survivor may submit a connected vehicle service request to the provider.

BACKGROUND

Related Bills

sSB 1295, favorably reported by the General Law Committee, among other things, has similar provisions to the ones in this bill that (1) change the knowledge standard for determining whether a consumer is a minor and (2) eliminate the option for anyone to consent to allow controllers that offer online services, products, or features to minors to perform certain actions, thus prohibiting the controllers from taking such actions.

HB 5474 (File 184), favorably reported by the Committee on Children, among other things, adds additional protection for minors using social media platforms by (1) requiring social media platform owners to incorporate an online safety center and establish a cyberbullying policy for handling cyber bullying reports on the platform and (2) expanding the CTDPA to include additional safeguards (e.g., avoiding harm to a minor's physical or mental health).

sHB 6002, favorably reported by the Government Administration and Elections Committee, removes provisions that exempt the state from the CTDPA.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 16 Nay 5 (03/21/2025)