Senate

General Assembly

File No. 604

January Session, 2023

Substitute Senate Bill No. 3

Senate, April 17, 2023

The Committee on Judiciary reported through SEN. WINFIELD of the 10th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

AN ACT CONCERNING ONLINE PRIVACY, DATA AND SAFETY PROTECTIONS.

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

Section 1. (NEW) (*Effective July 1, 2025*) (a) For the purposes of this section, unless the context otherwise requires:

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

(2) "Affiliate" means any legal entity that (A) shares common branding with another legal entity, and (B) controls, is controlled by or is under common control with another legal entity through (i) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting securities in either legal entity, (ii) control over the election of a majority of the directors of either legal entity or individuals exercising similar functions of the directors of either legal entity, or (iii) the power to exercise a controlling influence over the management of either legal entity;

(3) "Biometric data" has the same meaning as provided in section 42-515 of the general statutes;

(4) "Collect" means to buy, rent, access, retain, receive, acquire, infer, derive or otherwise process consumer health data in any manner;

(5) "Consent" has the same meaning as provided in section 42-515 of the general statutes;

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

(7) "Consumer health data" (A) means any personal information that is linked, or reasonably linkable, to a consumer and identifies the consumer's past, present or future physical or mental health, including, but not limited to, any (i) individual health condition, treatment, status, disease or diagnosis, (ii) social, psychological, behavioral or medical intervention, (iii) health-related surgery or procedure, (iv) use or purchase of medication, (v) bodily function, vital sign or symptom or any measurement of any such function, sign or symptom, (vi) diagnosis or diagnostic testing, treatment or medication, (vii) gender-affirming care information, (viii) reproductive or sexual health information, (ix) biometric data concerning the information described in this subparagraph, (x) genetic data concerning the information described in this subparagraph, (xi) precise location information that could reasonably indicate such consumer's attempt to acquire or receive health services or supplies, or (xii) information described in subparagraphs (A)(i) to (A)(xi), inclusive, of this subdivision that is derived or extrapolated from non-health information such as proxy, derivative, inferred or emergent data derived or extrapolated by any means, including, but not limited to, algorithms or machine learning, and (B) does not include any personal information that is used to engage in any public or peer-reviewed scientific, historical or statistical research, provided such research (i) is in the public interest, (ii) adheres to all other applicable ethics and privacy laws, and (iii) is approved, monitored and governed by an institutional review board, human subjects research ethics review board or another similar independent

oversight entity that determines that the regulated entity has implemented reasonable safeguards to mitigate privacy risks associated with such research, including, but not limited to, any risks associated with re-identification;

(8) "De-identified data" has the same meaning as provided in section 42-515 of the general statutes;

(9) "Gender-affirming care information" means any personal information concerning seeking or obtaining past, present or future gender-affirming care services, including, but not limited to, (A) any precise location information that could reasonably indicate a consumer's attempt to seek or obtain gender-affirming care services, (B) any personal information concerning any effort made to research or obtain gender-affirming care services, or (C) any gender-affirming care information that is derived, extrapolated or inferred, including, but not limited to, any such information that is derived, extrapolated or inferred from non-health information such as proxy, derivative, inferred, emergent or algorithmic data;

(10) "Gender-affirming care services" (A) means health services or products that support and affirm any consumer's gender identity, including, but not limited to, social, psychological, behavioral, cosmetic, medical or surgical interventions, and (B) includes, but is not limited to, treatments for gender dysphoria, gender-affirming hormone therapy and gender-affirming surgical procedures;

(11) "Genetic data" means any data, regardless of format, concerning a consumer's genetic characteristics and includes, but is not limited to, (A) raw sequence data that result from the sequencing of a consumer's complete extracted DNA or a portion of such extracted DNA, (B) genotypic and phenotypic information that results from analyzing such raw sequence data, and (C) self-reported health data that a consumer submits to a regulated entity and is analyzed in connection with such raw sequence data;

(12) "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 that is within two thousand feet of the perimeter around any physical location;

(13) "Health care service" means any service provided to any consumer to assess, measure, improve or learn about such consumer's health, including, but not limited to, any service provided to assess, measure, improve or learn about any (A) individual health condition, status, disease or diagnosis, (B) social, psychological, behavioral or medical intervention, (C) health-related surgery or procedure, (D) use or purchase of medication, (E) bodily function, vital sign or symptom or any measurement of any such function, sign or symptom, (F) diagnosis or diagnostic testing, treatment or medication, (G) reproductive or sexual health service, or (H) gender-affirming care services;

(14) "Person" means any individual, corporation, trust, unincorporated association or partnership, but does not include any government agency, tribal nation government organization or contracted service provider when such service provider is processing consumer health data on behalf of a government agency;

(15) "Personal information" (A) means any information that identifies, or is reasonably capable of being associated or linked, directly or indirectly, with any consumer, (B) includes, but is not limited to, any data associated with a persistent unique identifier such as an Internet browser cookie, Internet protocol address, device identifier or any other form of persistent unique identifier, and (C) does not include any publicly available information or de-identified data;

(16) "Precise location information" has the same meaning as provided in section 42-515 of the general statutes;

(17) "Process" and "processing" mean any operation or set of operations performed on consumer health data;

(18) "Processor" has the same meaning as provided in section 42-515 of the general statutes;

(19) "Publicly available information" has the same meaning as provided in section 42-515 of the general statutes;

(20) "Regulated entity" (A) means any legal entity that (i) does business in this state or produces or provides goods or services that are targeted to consumers in this state, and (ii) alone or jointly with others, determines the purpose and means of collecting, processing, sharing or selling consumer health data, and (B) does not mean any government agency, tribal nation government organization or contracted service provider when such service provider is processing consumer health data on behalf of a government agency;

(21) "Reproductive or sexual health information" (A) means any personal information concerning seeking or obtaining past, present or future reproductive or sexual health services, and (B) includes, but is not limited to, (i) any precise location information that could reasonably indicate a consumer's attempt to acquire or receive reproductive or sexual health services, (ii) any personal information concerning any effort made to research or obtain reproductive or sexual health services, and (iii) any personal information or location information described in this subdivision that is derived, extrapolated or inferred, including, but not limited to, any such information that is derived, extrapolated or inferred from any non-health information such as proxy, derivative, inferred, emergent or algorithmic data;

(22) "Reproductive or sexual health service" means any health service or product that supports or concerns any consumer's reproductive system or sexual well-being, including, but not limited to, any health service or product that supports or concerns any (A) individual health condition, status, disease or diagnosis, (B) social, psychological, behavioral or medical intervention, (C) health-related surgery or procedure, including, but not limited to, an abortion, (D) use or purchase of any medication, including, but not limited to, any medication used or purchased for the purposes of an abortion, (E)

bodily function, vital sign or symptom or any measurement of any such function, sign or symptom, (F) diagnosis or diagnostic testing, treatment or medication, and (G) medical or nonmedical service concerning and provided in conjunction with an abortion, including, but not limited to, any diagnostics, counseling, supplies and follow-up services concerning and provided in conjunction with an abortion;

(23) "Sale" or "sell" (A) means sharing consumer health data for monetary or other valuable consideration, and (B) does not include sharing consumer health data for monetary or other valuable consideration (i) to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the regulated entity's assets and complies with the requirements established in this section, or (ii) by a regulated entity to a processor when sharing such consumer health data is consistent with the purpose for which the consumer health data was collected and disclosed to the consumer;

(24) "Service provider" means any person that processes consumer health data on behalf of a regulated entity;

(25) "Share" and "sharing" (A) mean any release, disclosure, dissemination, divulsion, making available, provision of access to, licensing or communication, orally, in writing or by electronic or any other means, of consumer health data by a regulated entity to a third party or affiliate, and (B) do not include (i) any disclosure of consumer health data by a regulated entity to a processor if such disclosure is to provide goods or services in a manner that is consistent with the purpose for which such data was collected and disclosed to the consumer, (ii) any disclosure of consumer health data made to a third party with whom the consumer has a direct relationship when (I) such disclosure is made for the purpose of providing a product or service requested by such consumer, (II) the regulated entity maintains control and ownership of such data, and (III) the third party exclusively uses such data at the regulated entity's direction and in a manner that is consistent with the purpose for which such data was collected and

disclosed to the consumer, or (iii) any disclosure or transfer of consumer health data made to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the regulated entity's assets and complies with the requirements established in this section; and

(26) "Third party" means any entity other than a consumer, regulated entity or affiliate of a regulated entity.

(b) Notwithstanding any provision of the general statutes, each regulated entity shall:

(1) Restrict access to consumer health data by the employees, processors and contractors of such regulated entity:

(A) To those employees, processors and contractors for which the consumer to whom such data relates has provided consent; or

(B) Where such access is necessary to provide to the consumer to whom such data relates a product or service that such consumer has requested from such regulated entity;

(2) Establish, implement and maintain administrative, technical and physical data security practices that, at a minimum, satisfy a reasonable standard of care within such regulated entity's industry to protect the confidentiality, integrity and accessibility of consumer health data in a manner that is appropriate for the volume and nature of such consumer health data; and

(3) (A) Not collect or share consumer health data concerning any consumer (i) without having first obtained such consumer's consent to collect or share such consumer health data for a specified purpose, (ii) beyond what is reasonably necessary, proportionate and limited to provide or maintain (I) a specific product or service requested by such consumer, or (II) any communication by such regulated entity to such consumer that is reasonably anticipated within the context of their relationship, or (iii) for any purpose that is not expressly permitted under the provisions of this section.

(B) The consent required under subparagraph (A) of this subdivision shall (i) be separately and distinctly obtained for collecting and sharing consumer health data, and (ii) clearly and conspicuously disclose (I) the categories of consumer health data collected or shared, (II) the purpose of collecting or sharing the consumer health data, including, but not limited to, the specific ways in which such consumer health data will be used, (III) the categories of entities with which the consumer health data will be shared, and (IV) how the consumer may withdraw consent from any future collection or sharing of such consumer's consumer health data.

(c) (1) Notwithstanding any provision of the general statutes, no person shall:

(A) Sell, or offer to sell, consumer health data without first obtaining the consumer's signed, written consent on a form described in subdivision (2) of this subsection; or

(B) Implement a geofence to identify, track, collect data from or send notifications or messages to a consumer that enters the virtual perimeter around a health care provider or health care facility providing health care services on an in-person basis.

(2) Prior to selling, or offering to sell, a consumer's consumer health data, the person who intends to sell, or offer to sell, such consumer health data shall provide to the consumer a form containing:

(A) A description of the consumer health data to be offered or sold;

(B) The name of, and contact information for, the person who collected and intends to sell, or offer to sell, such consumer health data;

(C) The name of, and contact information for, the person who intends to purchase such consumer health data from the person described in subparagraph (B) of this subdivision;

(D) A description of the purpose of such proposed offer or sale, including, but not limited to, a description of how such consumer health

data will be gathered and how the person described in subparagraph (C) of this subdivision intends to use such consumer health data;

(E) A statement disclosing that the provision of goods or services shall not be made conditional on such consumer signing such form;

(F) A statement disclosing that such consumer has a right to revoke such consumer's consent at any time and a description of how such consumer may revoke such consent;

(G) A statement disclosing that any consumer health data sold pursuant to this subsection may be subject to redisclosure by the person described in subparagraph (C) of this subdivision and may no longer be protected under this section following such redisclosure;

(H) An expiration date for such consent, which date shall be not later than one year after such consumer signs such form; and

(I) Such consumer's signature and the date on which such consumer signs such form.

(3) No form required under subparagraph (A) of subdivision (1) of this subsection shall be valid if:

(A) The expiration date on such form has passed;

(B) Such form does not satisfy the requirements established in subdivision (2) of this subsection;

(C) The consumer has revoked such consumer's consent;

(D) Such form has been combined with any other document for the purpose of obtaining consent concerning multiple sales, or offers to sell, consumer health data; or

(E) The provision of goods or services is conditioned on the consumer signing such form.

(4) Each person who provides a form to a consumer pursuant to

subdivision (2) of this subsection shall provide a signed copy of such form to the consumer who signed such form.

(5) Each person who sells or purchases consumer health data in the manner described in this subsection shall retain a copy of each form required under subdivision (2) of this subsection for a period of at least six years beginning on the date the consumer signed such form or the last date such form was effective, whichever is later.

(d) A processor may process consumer health data only pursuant to a binding contract between the processor and a regulated entity, which contract shall set forth the processing instructions for, and limit the actions which the processor may take with respect to, the consumer health data such processor processes on behalf of the regulated entity. The processor shall not process consumer health data in a manner that is inconsistent with the terms of such contract. The processor shall assist the regulated entity by taking all appropriate and possible technical and organizational measures that are necessary for such regulated entity to perform such regulated entity's duties under this section. If the processor fails to adhere to the regulated entity's processing instructions or processes consumer health data in a manner that is outside the scope of such contract, such processor shall be deemed to constitute a regulated entity and shall be subject to all provisions of this section concerning regulated entities.

(e) Any violation of the provisions of this section shall constitute an unfair trade practice under subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. Nothing in this section shall be construed to create a private right of action or to provide grounds for an action under section 42-110g of the general statutes.

Sec. 2. (NEW) (*Effective July 1, 2024*) (a) For the purposes of this section:

(1) "Consumer" has the same meaning as provided in section 42-515 of the general statutes;

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

(3) "Personal data" has the same meaning as provided in section 42-515 of the general statutes; and

(4) "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, or (ii) primarily consists of news, sports, entertainment, 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.

(b) Not later than ten days after a social media platform receives a request to delete a social media platform account from a minor or, if the minor is younger than sixteen years of age, from a minor's parent or legal guardian, the social media platform shall delete the minor's social media platform account and cease processing such minor's personal data. 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.

(c) No social media platform shall establish an account for a minor who is younger than sixteen years of age unless the social media platform has obtained consent from the minor's parent or legal guardian to establish such account.

(d) Any violation of the provisions of this section shall constitute an unfair trade practice under subsection (a) of section 42-110b of the general statutes and shall be enforced solely by the Attorney General. Nothing in this section shall be construed to create a private right of action or to provide grounds for an action under section 42-110g of the general statutes.

Sec. 3. (NEW) (*Effective July 1, 2025*) For the purposes of this section and sections 4 to 8, inclusive, of this act:

(1) "Adult" means any individual who is at least eighteen years of age;

(2) "Algorithm" means any computerized procedure consisting of a set of steps used to accomplish a predetermined objective;

(3) "Consent" has the same meaning as provided in section 42-515 of the general statutes;

(4) "Consumer" has the same meaning as provided in section 42-515 of the general statutes;

(5) "Controller" means any person that, alone or jointly with others, determines the purpose and means of processing personal data;

(6) "Heightened risk of harm to minors" means processing minors' personal data, including, but not limited to, through use of any algorithm, in a manner that presents any reasonably foreseeable risk of (A) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors, (B) any financial, physical or reputational injury to minors, (C) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person, or (D) any other substantial injury to minors;

(7) "HIPAA" has the same meaning as provided in section 42-515 of the general statutes;

(8) "Minor" means any consumer who is younger than eighteen years

of age;

(9) "Online service, product or feature" means any service, product or feature that is provided online. "Online service, product or feature" does not include any (A) telecommunications service, as defined in 47 USC 153, as amended from time to time, or (B) delivery or use of a physical product;

(10) "Person" means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship or trust;

(11) "Personal data" has the same meaning as provided in section 42-515 of the general statutes;

(12) "Precise geolocation data" has the same meaning as provided in section 42-515 of the general statutes;

(13) "Process" and "processing" have the same meaning as provided in section 42-515 of the general statutes;

(14) "Processor" means any person that, on behalf of a controller, processes personal data;

(15) "Profiling" has the same meaning as provided in section 42-515 of the general statutes;

(16) "Protected health information" has the same meaning as provided in section 42-515 of the general statutes;

(17) "Sale of personal data" has the same meaning as provided in section 42-515 of the general statutes;

(18) "Targeted advertising" (A) means displaying an advertisement to a minor based on profiling, and (B) does not include (i) an advertisement that is (I) based on the context of a minor's current search query, visit to an Internet web site or online application, or (II) directed to a minor in response to the minor's current request for information or feedback, or (ii) processing personal data solely to measure or report advertising frequency, performance or reach; and

(19) "Third party" has the same meaning as provided in section 42-515 of the general statutes.

Sec. 4. (NEW) (*Effective July 1, 2025*) (a) Each controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall use reasonable care to avoid any heightened risk of harm to minors proximately caused by such online service, product or feature.

(b) (1) Subject to the consent requirement established in subdivision (3) of this subsection, no controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall process any minor's personal data: (A) For the purposes of (i) targeted advertising, (ii) any sale of personal data, or (iii) profiling in furtherance of any decision made by such controller that results in the provision or denial by such controller of any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services; (B) that is not reasonably necessary to provide such online service, product or feature; (C) for any processing purpose other than the purpose that the controller disclosed at the time such controller collected such personal data; (D) for longer than is reasonably necessary to provide such online service, product or feature; or (E) in any circumstances in which such minor's personal data is accessible by, or visible to, any other user of such online service, product or feature.

(2) Subject to the consent requirement established in subdivision (3) of this subsection, no controller that offers an online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall collect a minor's precise geolocation data unless: (A) Such precise geolocation data is necessary for the controller to provide such online service, product or feature and, if such data is 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 conspicuous 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) No controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors shall: (1) Use any user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, including, but not limited to, any practice the Federal Trade Commission refers to as a "dark pattern", to lead or encourage any minor to provide any personal data that is not reasonably necessary to provide such online service, product or feature; (2) by default use any system design feature to increase, sustain or extend any minor's use of such online service, product or feature by, among other things, automatically playing any media, offering any reward to encourage such minor to spend time using such online service, product or feature or sending notifications to such minor; (3) allow any minor's parent, legal guardian or any other consumer to monitor such minor's online activity unless such controller provides to such minor a signal, which is obvious to such minor, indicating that such minor is being monitored; or (4) allow any adult to contact any minor through any messaging apparatus unless such adult previously established and maintains an ongoing lawful relationship with such minor.

Sec. 5. (NEW) (*Effective July 1, 2025*) (a) Each controller that, on or after July 1, 2025, offers any online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, 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 of the general statutes; 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.

(b) Each controller that conducts a data protection assessment pursuant to subsection (a) of this section shall: (1) Review such data protection assessment at least biennially; and (2) maintain documentation concerning such data protection assessment as long as such controller offers the online service, product or feature that is the subject of such assessment to minors.

(c) If any controller conducts a data protection assessment pursuant to subsection (a) of this section and determines that the online service, product or feature that is the subject of such assessment poses a heightened risk of harm to minors, such controller shall establish and implement a plan to mitigate or eliminate such risk before such controller offers such online service, product or feature to consumers whom such controller has actual knowledge, or wilfully disregards, are minors.

Sec. 6. (NEW) (*Effective July 1, 2025*) (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 3 to 8, inclusive, of this act. Such assistance shall include providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the

processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that the processor: (1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; (2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 3 to 8, inclusive, of this act; (4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 3 to 8, inclusive, of this act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in sections 3 to 8, inclusive, of this act.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to

adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under section 8 of this act.

Sec. 7. (NEW) (*Effective July 1, 2025*) (a) The provisions of sections 1, 3 to 6, inclusive, and 8 of this act shall 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) 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; (3) 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; (4) national securities association that is registered under 15 USC 78o-3, as amended from time to time; (5) financial institution or data that is subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., as amended from time to time; (6) covered entity or business associate, as defined in 45 CFR 160.103, as amended from time to time; or (7) 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, 49 USC 41713, as said acts may be amended from time to time.

(b) The following information and data is exempt from the provisions of sections 1, 3 to 6, inclusive, and 8 of this act: (1) Protected health information; (2) patient-identifying information for the purposes of 42 USC 290dd-2, as amended from time to time; (3) identifiable private information for the purposes of the federal policy for the protection of human subjects under 45 CFR 46, as amended from time to time; (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 Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, as amended from time to time; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, as amended from time to time, or personal data used or shared in research, as defined in 45 CFR 164.501, as amended from time to time, 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 the purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq., as amended from time to time; (7) patient safety work products for the purposes of section 19a-127o of the general statutes 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 under HIPAA; (9) information originating from and intermingled so as to be indistinguishable from, or information treated in the same manner as, information that is exempt under this subsection and 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 or third party, to the extent that the data is collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 1, 3 to 6, inclusive, and 8 of 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 Airline Deregulation Act, 49 USC 40101 et seq., as amended from time to time, by an air carrier subject to said act, to the extent sections 1, 3 to 6, inclusive, and 8 of this act are preempted by 49 USC 41713, as amended from time to time.

(c) No provision of this section or section 1, 3 to 6, inclusive, or 8 of this act shall be construed to restrict a controller's or processor'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 or processor 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) take immediate steps to protect an interest that is essential for the life or physical safety of the minor or another individual, and where the processing cannot be manifestly based on another legal basis; (6) 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; (7) 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 processor, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller or processor has implemented reasonable safeguards to mitigate privacy risks associated with research, including, but not limited to, any risks associated with re-identification; (8) assist another controller, processor or third party with any obligation under section 1, 3 to 6, inclusive, or 8 of this act; or (9) 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 minor whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(d) No obligation imposed on a controller or processor under any provision of section 1, 3 to 6, inclusive, or 8 of this act 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 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.

(e) No controller or processor shall be required to comply with any provision of section 1, 3 to 6, inclusive, or 8 of this act if compliance with such provision would violate an evidentiary privilege under the laws of this state, and no such provision shall be construed to prevent a

controller or processor from providing, as part of a privileged communication, any personal data concerning a minor to any other person who is covered by such evidentiary privilege.

(f) No provision of section 1, 3 to 6, inclusive, or 8 of this act shall be construed to: (1) Impose any obligation on a controller that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person (A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or (B) under section 52-146t of the general statutes; or (2) apply to any individual's processing of personal data in the course of such individual's purely personal or household activities.

(g) (1) Any personal data processed by a controller pursuant to this section may be processed to the extent that such processing is: (A) Reasonably necessary and proportionate to the purposes listed in this section; and (B) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section.

(2) Any controller that collects, uses or retains data pursuant to subsection (d) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to minors concerning such collection, use or retention of personal data.

(h) If any controller or processor processes personal data pursuant to an exemption established in subsections (a) to (g), inclusive, of this section, such controller or processor bears the burden of demonstrating that such processing qualifies for such exemption and complies with the requirements established in subsection (g) of this section.

Sec. 8. (NEW) (*Effective July 1, 2025*) (a) Any violation of the provisions of sections 3 to 7, inclusive, of this act shall constitute an unfair trade practice under subsection (a) of section 42-110b of the

general statutes and shall be enforced solely by the Attorney General. Nothing in this section or sections 3 to 7, inclusive, of this act shall be construed to create a private right of action or to provide grounds for an action under section 42-110g of the general statutes.

(b) (1) During the period beginning July 1, 2025, and ending December 31, 2027, if the Attorney General, in the Attorney General's discretion, determines that a controller or processor has violated any provision of sections 3 to 7, inclusive, of this act but may cure such alleged violation, the Attorney General shall provide written notice to such controller or processor, in a form and manner prescribed by the Attorney General and before the Attorney General commences any action to enforce such provision, disclosing such alleged violation and such provision.

(2) (A) Not later than thirty days after a controller or processor receives a notice under subdivision (1) of this subsection, the controller or processor may send a notice to the Attorney General, in a form and manner prescribed by the Attorney General, disclosing that such controller or processor has: (i) Determined that such controller or processor did not commit the alleged violation of sections 3 to 7, inclusive, of this act; or (ii) cured such violation and taken measures that are sufficient to prevent further such violations.

(B) If the Attorney General receives a notice described in subparagraph (A) of this subdivision and determines, in the Attorney General's discretion, that the controller or processor that sent such notice did not commit the alleged violation or has cured such violation and taken the measures described in subparagraph (A)(ii) of this subdivision, such controller or processor shall not be liable for any civil penalty under subsection (a) of this section.

(C) Not later than February 1, 2027, the Attorney General shall submit a report, in accordance with section 11-4a of the general statutes, to the joint standing committee of the General Assembly having cognizance of matters relating to general law. Such report shall disclose: (i) The number of notices the Attorney General has issued pursuant to

subdivision (1) of this subsection; (ii) the nature of each violation that was the subject of a notice issued by the Attorney General pursuant to subdivision (1) of this subsection; (iii) the number of violations that were cured pursuant to subparagraphs (A) and (B) of this subdivision; and (iv) any other matter the Attorney General deems relevant for the purposes of such report.

(c) Beginning on January 1, 2027, the Attorney General may, in the Attorney General's discretion, provide to a controller or processor an opportunity to cure any alleged violation of the provisions of sections 3 to 7, inclusive, of this act in the manner described in subdivisions (1) and (2) of section (b) of this section. In determining whether to grant the controller or processor an opportunity to cure such alleged violation, the Attorney General may consider: (1) The number of such violations that such controller or processor is alleged to have committed; (2) the size and complexity of such controller or processor; (3) the nature and extent of such controller's or processor's processing activities; (4) whether there exists a substantial likelihood that such alleged violation has caused or will cause public injury; (5) the safety of persons or property; and (6) whether such alleged violation was likely caused by a human or technical error.

Sec. 9. Section 54-33c of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2023*):

(a) The applicant for a search warrant shall file the application for the warrant and all affidavits upon which the warrant is based with the clerk of the court for the geographical area within which any person who may be arrested in connection with or subsequent to the execution of the search warrant would be presented with the return of the warrant. Upon the arrest of any person in connection with or subsequent to the execution of the search warrant, the law enforcement agency that arrested the person shall notify the clerk of such court of the return of the warrant by completing a form prescribed by the Chief Court Administrator and filing such form with the clerk together with any applicable uniform arrest report or misdemeanor summons.

(b) Except for a warrant for the installation and use of a tracking device: (1) The warrant shall be executed within ten days and returned with reasonable promptness consistent with due process of law and shall be accompanied by a written inventory of all property seized; (2) a copy of such warrant shall be given to the owner or occupant of the dwelling, structure, motor vehicle or place designated in the warrant, or the person named in the warrant; and (3) within forty-eight hours of such search, a copy of the application for the warrant and a copy of all affidavits upon which the warrant is based shall be given to such owner, occupant or person. The judge or judge trial referee may, by order, dispense with the requirement of giving a copy of the affidavits to such owner, occupant or person at such time if the applicant for the warrant files a detailed affidavit with the judge or judge trial referee which demonstrates to the judge or judge trial referee that (A) the personal safety of a confidential informant would be jeopardized by the giving of a copy of the affidavits at such time, or (B) the search is part of a continuing investigation which would be adversely affected by the giving of a copy of the affidavits at such time, or (C) the giving of a copy of the affidavits at such time would require disclosure of information or material prohibited from being disclosed by chapter 959a. If a warrant is directed to a provider of an electronic communication service or a remote computing service, as such terms are defined in subsection (a) of section 54-47aa, for records of a subscriber or customer of such provider, the court shall order that the provider not disclose the existence of such warrant to such subscriber or customer or any other person or entity for a period of up to ninety days if the court determines that there is reason to believe that notification of the existence of the warrant may result in (i) endangering the life or physical safety of an individual, (ii) flight from prosecution, (iii) destruction of or tampering with evidence, (iv) intimidation of potential witnesses, or (v) otherwise seriously jeopardizing the investigation.

(c) A warrant for the installation and use of a tracking device shall be returned with reasonable promptness consistent with due process of law and after the period authorized for tracking, including any extension period authorized under subsection (d) of section 54-33a, has

expired. Within ten days after the use of the tracking device has ended, a copy of the application for the warrant and a copy of all affidavits upon which the warrant is based shall be given to the person who was tracked or the owner of the property to, in or on which the tracking device was installed. The judge or judge trial referee may, by order, dispense with the requirement of giving a copy of the affidavits to the person who was tracked or the owner of the property to, in or on which the tracking device was installed if the applicant for the warrant files a detailed affidavit with the judge or judge trial referee which demonstrates to the judge or judge trial referee that (1) the personal safety of a confidential informant would be jeopardized by the giving of a copy of the affidavits at such time, or (2) the search is part of a continuing investigation which would be adversely affected by the giving of a copy of the affidavits at such time, or (3) the giving of a copy of the affidavits at such time would require disclosure of information or material prohibited from being disclosed by chapter 959a.

(d) If the judge or judge trial referee dispenses with the requirement of giving a copy of the affidavits at such time pursuant to subsection (b) or (c) of this section, such order shall not affect the right of such owner, occupant or person to obtain such copy at any subsequent time. No such order shall limit the disclosure of such affidavits to the attorney for a person arrested in connection with or subsequent to the execution of a search warrant unless, upon motion of the prosecuting authority within two weeks of such person's arraignment, the court finds that the state's interest in continuing nondisclosure substantially outweighs the defendant's right to disclosure.

(e) Any order entered pursuant to subsection (b) or (c) of this section dispensing with the requirement of giving a copy of the affidavits to such owner, occupant or person shall be for a specific period of time, not to exceed (1) two weeks beyond the date the warrant is executed, or (2) with respect to a warrant for the installation and use of a tracking device, two weeks after any extension period authorized under subsection (d) of section 54-33a has expired. Within the applicable time period set forth in subdivision (1) or (2) of this subsection, the prosecuting authority

may seek an extension of such period of time. Upon the execution and return of the warrant, affidavits which have been the subject of such an order shall remain in the custody of the clerk's office in a secure location apart from the remainder of the court file.

Sec. 10. Section 21a-435 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2023*):

As used in this section, **[**and**]** sections 21a-436 to 21a-439, inclusive, and section 11 of this act:

(1) "Connecticut user" means a user who provides a Connecticut home address or zip code when registering with an online dating operator or a user who is known or determined by an online dating operator or its online dating platform to be in Connecticut at the time of registration;

(2) "Criminal background screening" means a name search for an individual's history of criminal convictions that is conducted by searching an (A) available and regularly updated government public record database that in the aggregate provides national coverage for searching an individual's history of criminal convictions; or (B) a regularly updated database maintained by a private vendor that provides national coverage for searching an individual's history of criminal convictions and sexual offender registries;

(3) "Criminal conviction" means a conviction for a crime in this state, another state, or under federal law;

(4) "Online dating" means the act of using a digital service to initiate relationships with other individuals for the purpose of romance, sex or marriage;

(5) "Online dating operator" means a person who operates a software application designed to facilitate online dating;

(6) "Online dating platform" means a digital service designed to allow users to interact through the Internet to participate in online dating; and

(7) "User" means an individual who uses the online dating services of an online dating operator.

Sec. 11. (NEW) (*Effective October 1, 2023*) An online dating operator shall owe a duty of care to any user of its online dating platform to protect against potential criminal activity of other users, including a duty to notify users if the online dating operator has had a communication with another user determined by the online dating operator to have a higher propensity to commit a crime against individuals.

Sec. 12. Section 29-7b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1, 2023*):

(a) There shall be within the Department of Emergency Services and Public Protection a Division of Scientific Services. The Commissioner of Emergency Services and Public Protection shall serve as administrative head of such division, and may delegate jurisdiction over the affairs of such division to a deputy commissioner.

(b) The Division of Scientific Services shall provide technical assistance to law enforcement agencies in the various areas of scientific investigation. The division shall maintain facilities and services for the examination and analysis of evidentiary materials in areas including, but not limited to, chemistry, arson, firearms, questioned documents, microscopy, serology, toxicology, trace evidence, latent fingerprints, impressions and other similar technology. The facilities, services and personnel of the division shall be available, without charge, to the Office of the Chief Medical Examiner and all duly constituted prosecuting, police and investigating agencies of the state.

(c) The Division of Scientific Services: (1) May investigate any physical evidence or evidentiary material related to a crime upon the request of any federal, state or local agency, (2) may conduct or assist in the scientific field investigation at the scene of a crime and provide other technical assistance and training in the various fields of scientific criminal investigation upon request, (3) shall assure the safe custody of

evidence during examination, (4) shall forward a written report of the results of an examination of evidence to the agency submitting such evidence, (5) shall render expert court testimony when requested, and (6) shall conduct ongoing research in the areas of the forensic sciences. The Commissioner of Emergency Services and Public Protection or a director designated by the commissioner shall be in charge of the Division of Scientific Services operations and shall establish and maintain a system of case priorities and a procedure for submission of evidence and evidentiary security. The director of the Division of Scientific Services shall be in the unclassified service and shall serve at the pleasure of the commissioner.

(d) In accordance with the provisions of sections 4-38d, 4-38e and 4-39, all powers and duties of the Department of Public Health under the provisions of sections 14-227a, 14-227c, 15-140u and 21a-283 shall be transferred to the Division of Scientific Services within the Department of Emergency Services and Public Protection.

(e) There is established within the Division of Scientific Services the Connecticut Internet Crimes Against Children Task Force, which shall consist of affiliate law enforcement agencies in the state. The task force shall use state and federal moneys appropriated to it in a manner that is consistent with the duties prescribed in 34 USC 21114.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*July 1, 2025*	New section
Sec. 2	*July 1, 2024*	New section
Sec. 3	*July 1, 2025*	New section
Sec. 4	*July 1, 2025*	New section
Sec. 5	*July 1, 2025*	New section
Sec. 6	*July 1, 2025*	New section
Sec. 7	*July 1, 2025*	New section
Sec. 8	*July 1, 2025*	New section
Sec. 9	*October 1, 2023*	54-33c
Sec. 10	*October 1, 2023*	21a-435
Sec. 11	*October 1, 2023*	New section

Sec. 12	*July 1, 2023*	29-7b

Statement of Legislative Commissioners:

In Section 1, Subsec. (a) was redrafted to remove the definition of the unused term "dark patterns" and, in Subsec. (a), Subdivs. (9) to (27), inclusive, were redesignated Subdivs. (8) to (26), inclusive, and Subdivs. (7)(A), (13), (21)(B)(ii) and (22) were redrafted for internal consistency, in Subsec. (b)(3)(B)(ii)(II), "of" was deleted for internal consistency, and in Subsec. (c)(2), "consumer health data" was changed to "consumer's consumer health data" for accuracy; and in Section 9(b)(3)(C), "electronic communications service as defined in subdivision (4) of subsection (a) of section 54-47aa, or a remote computing service in subdivision (8) of subsection (a) of section 54-47aa," was changed to "electronic communication service or a remote computing service, as such terms are defined in subsection (a) of section 54-47aa," for accuracy and conciseness.

JUD *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 24 $	FY 25 $
Attorney General	GF - Potential Revenue Gain	See Below	See Below

Note: GF=General Fund

Municipal Impact: None

Explanation

The bill may result in a revenue gain to the Office of the Attorney General (OAG) beginning in FY 24, as any violations of Sections 1, 2, and 4 – 6 are considered violations of the Connecticut Unfair Trade Practices Act (CUTPA), and enforced solely by OAG.

Any revenue gain would depend on the number and type of violations enforced by OAG. CUTPA allows OAG to seek various forms of relief to address violations, including penalties of up to $5,000 per willful violation. The agency could seek these penalties through an enforcement action, or if a company cooperates, through a settlement resolving the state's claims. For FY 20 – FY 22, annual revenue collected from CUTPA ranged from a low of $1,639,854 to $4,523,004.

Sections 1 - 2 prohibit anyone from selling consumer health data without obtaining the consumer's written consent. These sections also create a ban on anyone using a geofence to identify, track, collect data from or send notifications to a consumer entering a health care facility.[1]

[1]A "geofence" is 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.

Sections 3 – 8 establish a framework and set requirements regarding how those who offer online services and products manage, process, and obtain consent to use the personal data of minors.

Section 8 specifically allows the OAG, from July 1, 2025, to December 31, 2027, before initiating any enforcement action, to issue a written notice of violation to give the party an opportunity to cure the violation.

Section 12 creates the Connecticut Internet Crimes Against Children Task Force. Any costs to the state in FY 24 and FY 25 would depend on the level of any state and federal appropriations.

The Out Years

The annualized ongoing fiscal impact identified above would continue into the future subject to the number and extent of any violations enforced by OAG.

OLR Bill Analysis

sSB 3

AN ACT CONCERNING ONLINE PRIVACY, DATA AND SAFETY PROTECTIONS.

SUMMARY

This bill sets standards on accessing and sharing consumer health data by certain private entities that do business in Connecticut (§ 1). Among other things, these entities must limit access to consumer health data to individuals and situations specified in the bill. They are also prohibited from collecting or sharing this data without first getting a consumer's consent. The bill also prohibits anyone from selling this data unless a consumer has completed a particular consent form.

The bill also establishes a framework and sets requirements for how individuals or entities offering certain online services, products, and features manage and process personal data for minors (i.e., those under age 18) (§§ 4-6). It specifically requires them to use reasonable care to avoid having their services, products, and features proximately cause, among other things, substantial injury to a minor. They are also prohibited from (1) processing the minor's personal data without receiving the minor's or his or her parent's or guardian's consent and (2) collecting a minor's precise geolocation data.

Additionally, the bill prohibits certain social media platforms from establishing an account for a minor under age 16 without a parent's or guardian's consent (§ 2). It also requires these platforms to delete a minor's social media account and stop processing the minor's personal data within 10 days after getting a request to delete the account.

Under the bill, any violation of the consumer health data, online services, and social media provisions is deemed a violation under the Connecticut Unfair Trade Practices Act (CUTPA), enforced solely by the

attorney general (§§ 1, 2 & 4-6). It further specifies that none of its provisions may be construed to create a private right of action or grounds for an action under CUTPA.

The bill also:

1. allows courts to order that providers of electronic communication or remote computing services not disclose the existence of a warrant for subscriber or customer records to any person or entity for up to 90 days if a court determines certain exigent or security reasons exist (§ 9);

2. requires online dating operators to owe a duty of care to their users to protect them against potential criminal activity of other users (§§ 10 & 11); and

3. statutorily establishes the Connecticut Internet Crimes Against Children task force (CT ICAC) and requires it to use state and federal funding appropriated to it in a way that is consistent with its duties under federal law (§ 12).

EFFECTIVE DATE: July 1, 2025, except the CT ICAC provision is effective July 1, 2023, the warrant non-disclosure and online dating operator provisions are effective October 1, 2023, and the social media provision is effective July 1, 2024.

§ 1 — CONSUMER HEALTH DATA DEFINITIONS

The bill sets standards for how regulated entities access and share consumer health data.

Regulated Entity and Consumer

Under the bill, a "regulated entity" is any legal entity that (1) does business in Connecticut or produces or provides goods or services that are targeted to Connecticut consumers and (2) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling consumer health data. It does not include any government agency, tribal nation government organization, or

contracted service provider when the provider is processing consumer health data on behalf of a government agency.

The bill defines "consumer" as a state resident but excludes anyone acting (1) in a commercial or employment context or (2) 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 person's role with the entity (CGS § 42-515(7)).

Consumer Health Data Generally

For the purposes of the bill, "consumer health data" is any personal information that is linked, or reasonably linkable, to a consumer and identifies the consumer's past, present, or future physical or mental health.

"Personal information" is any information that identifies, or is reasonably capable of being associated or linked, directly or indirectly, with any consumer, including any data associated with a persistent unique identifier such as an Internet browser cookie, Internet protocol address, device identifier, or any other form of persistent unique identifier. It does not include any publicly available information or de-identified data.

"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 a consumer has lawfully made available to the general public (CGS § 42-515(25)). (By law, a "controller" is an individual or legal entity that, alone or jointly with others, determines the purpose and means of processing "personal data" (i.e., any information that is linked, or reasonably linkable, to an identified or identifiable individual, excluding de-identified data or publicly available information) (CGS § 42-515(8) & (18)).)

"De-identified data" is data that cannot reasonably be used to infer information about, or otherwise be linked to, a specific individual or his

or her device. To be de-identified, a controller that possesses the data must (1) take reasonable measures to ensure the data cannot be associated with the individual, (2) publicly commit to process the data only in a de-identified fashion and not attempt to re-identify the data, and (3) contractually obligate anyone receiving the data to satisfy these requirements (CGS § 42-515(13)).

Consumer Health Data Inclusions

"Consumer health data" specifically includes any personal information that identifies a consumer's:

1. individual health condition, treatment, status, disease, or diagnosis;
2. social, psychological, behavioral, or medical intervention;
3. health-related surgery or procedure;
4. medication use or purchase;
5. bodily function, vital sign, or symptom (or measurement of any of them);
6. diagnosis or diagnostic testing, treatment, or medication;
7. "gender-affirming care information" (see below);
8. "reproductive or sexual health information" (see below);
9. biometric and genetic data (see below); and
10. "precise location information" (see below) that could reasonably show the consumer's attempt to acquire or receive health services or supplies.

It also includes any information described above that is derived or extrapolated from non-health information such as proxy, derivative, inferred or emergent data derived or extrapolated by any means, including algorithms or machine learning.

Gender-Affirming Care Information and Services. Under the bill, "gender-affirming care information" is any personal information about seeking or getting, past, present, or future gender-affirming care services, including any of the following:

1. precise location information that could reasonably indicate a consumer's attempt to seek or obtain these services;

2. personal information on any effort made to research or get these services; and

3. information that is derived, extrapolated, or inferred, including from non-health information such as proxy, derivative, inferred, emergent, or algorithmic data.

"Gender-affirming care services" are health services or products that support and affirm any consumer's gender identity, including social, psychological, behavioral, cosmetic, medical, or surgical interventions. They include (1) treatments for gender dysphoria, (2) gender-affirming hormone therapy, and (3) gender-affirming surgical procedures.

Reproductive or Sexual Health Information and Services. For the purposes of the bill, "reproductive or sexual health information" is any personal information about seeking or getting past, present, or future reproductive or sexual health services, including:

1. precise location information that could reasonably show a consumer's attempt to acquire or receive these services;

2. personal information about any effort made to research or obtain these services; and

3. personal information or location information that is derived, extrapolated, or inferred, including from non-health information such as proxy, derivative, inferred, emergent, or algorithmic data.

"Reproductive or sexual health service" is any health service or

product that supports or concerns any consumer's reproductive system or sexual well-being, including any that support or concern any:

1. individual health condition, status, disease, or diagnosis;
2. social, psychological, behavioral, or medical intervention;
3. health-related surgery or procedure, including an "abortion" (i.e., terminating a pregnancy for any purpose other than producing a live birth);
4. medication use or purchase, including any for the purposes of an abortion;
5. bodily function, vital sign, or symptom (or measurement of any of them);
6. diagnosis or diagnostic testing, treatment, or medication; and
7. medical or nonmedical service about and provided in conjunction with an abortion, including any diagnostics, counseling, supplies, and follow-up services related to an abortion.

Biometric Data. Under the bill, "biometric data" is data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or identifying characteristics. It does not include digital or physical photographs, video or audio recordings, or data generated from these, unless the data is generated to identify a specific individual (CGS § 42-515(3)).

Genetic Data. For the purposes of the bill, "genetic data" is any data, regardless of format, about a consumer's genetic characteristics including (1) raw sequence data from sequencing all or a portion of a consumer's extracted DNA, (2) genotypic and phenotypic information from analyzing the raw sequence data, and (3) self-reported health data that a consumer submits to a regulated entity and is analyzed in

connection with the raw sequence data.

Precise Location Information. Presumably, under the bill, "precise location information" has the same meaning as "precise geolocation data" under existing law, which is information derived from technology, including 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 1,750 feet. It excludes the content of communications, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility (CGS § 42-515(19)).

Consumer Health Data Exclusions

"Consumer health data" does not include any personal information that is used to engage in any public or peer-reviewed scientific, historical or statistical research if the research (1) is in the public interest, (2) adheres to all other applicable ethics and privacy laws, and (3) is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or another similar independent oversight entity that determines that the regulated entity has implemented reasonable safeguards to mitigate privacy risks associated with the research, including any risks associated with re-identification.

"Process" or "processing" means any manual or automatic operation or set of operations performed on personal data or sets of personal data, including collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data.

§ 1 — CONSUMER HEALTH DATA MANAGEMENT

Access and Security to Consumer Health Data (§ 1(b)(1) & (2))

Regardless of any other state law, the bill requires regulated entities to restrict access to consumer health data by their employees, processors, and contractors to those, presumably, (1) who the consumer has provided consent to access his or her data or (2) where the access is

needed to provide a product or service that the consumer has requested from the regulated entity.

Under the bill, "processors" are those who process "personal data" for a "controller" (see above) (CGS § 42-515(21)). Additionally, "consent" is a clear affirmative act signifying the consumer's informed agreement to allow the processing of his or her personal data, including by written statement, which may be electronic. It does not include (1) accepting a general or broad terms of use or similar document that contains personal data processing descriptions along with other, unrelated information; (2) hovering over, muting, pausing, or closing a given piece of content; or (3) obtaining agreement through the use of dark patterns (CGS § 42-515(6)). A "dark pattern" (1) is a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice and (2) includes any practice the Federal Trade Commission refers to as a "dark pattern" (CGS § 42-515(11)).

The bill also requires, regardless of any other state law, each regulated entity must establish, implement, and maintain administrative, technical, and physical data security practices which must at least satisfy a reasonable standard of care within the regulated entity's industry to protect the confidentiality, integrity, and accessibility of consumer health data in an appropriate manner for the volume and nature of the consumer health data.

Prohibition on Collecting and Sharing Consumer Health Data (§ 1(b)(3))

Regardless of any other state law, the bill prohibits regulated entities from collecting or sharing consumer health data about any consumer:

1. without first obtaining his or her consent to do so for a specified purpose;

2. beyond what is reasonably needed, proportionate, and limited to provide or maintain (a) a specific product or service the consumer requested or (b) any communication by the entity to

the consumer that is reasonably anticipated within the context of their relationship; or

3. for any purpose that is not expressly allowed under the bill's consumer health data provisions.

Under the bill, "collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any way.

Additionally, "share" and "sharing" mean any release, disclosure, dissemination, divulsion, making available, access given, licensing, or oral or written communications of consumer health data by a regulated entity to a third party or affiliate. It excludes any disclosure of consumer health data:

1. by a regulated entity to a processor if the disclosure is to provide goods or services in a way that is consistent with the purpose for which the data was collected and disclosed to the consumer; and

2. made to a third party with whom the consumer has a direct relationship when the (a) disclosure is made for the purpose of providing a product or service requested by the consumer, (b) regulated entity maintains control and ownership of the data, and (c) the third party exclusively uses the data at the regulated entity's direction and in a way that is consistent with the purpose for which the data was collected and disclosed to the consumer.

The bill further excludes any disclosure or transfer of consumer health data made to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's assets and complies with the requirements established in the bill's consumer health data provisions.

Under the bill, a "third party" is any entity other than a consumer, regulated entity, or a regulated entity's affiliate. An "affiliate" is any legal entity that (1) shares common branding with another legal entity,

and (2) controls, is controlled by, or is under common control with another legal entity through (a) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting securities in either legal entity, (b) control over the election of a majority of the directors of either legal entity or people exercising similar directorial functions of either legal entity, or (c) the power to exercise a controlling influence over the management of either legal entity.

For the purposes of the above prohibition, required consent must, in addition to what is required under its definition, be separately and distinctly obtained for collecting and sharing consumer health data and clearly and conspicuously disclose:

1. the categories of consumer health data collected or shared;

2. the purpose of collecting or sharing the consumer health data, including the specific ways the consumer health data will be used;

3. the categories of entities the consumer health data will be shared with; and

4. how the consumer may withdraw consent from any future collection or sharing of the consumer's consumer health data.

Prohibition on Selling Consumer Health Data (§ 1(c)(1)(A) & (2))

Regardless of any other state law, the bill prohibits anyone from selling, or offering to sell, consumer health data without first getting the consumer's signed, written consent on a specified form. Under the bill, "sale or sell" is sharing consumer health data for monetary or other valuable consideration, except:

1. to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's assets and complies with the requirements in the bill's consumer health data provisions; or

2. by a regulated entity to a processor when sharing the consumer health data is consistent with the purpose for which the consumer health data was collected and disclosed to the consumer.

The form that must be given to consumers before selling or offering to sell their health data must contain:

1. a description of the consumer health data to be offered or sold;

2. the name and contact information for the people who (a) collected and intend to sell, or offer to sell, the consumer health data and (b) intend to buy the data from the collector;

3. a description of the purpose of the proposed offer or sale, including a description of how the consumer health data will be gathered and how the person intending to buy the data plans to use it;

4. statements disclosing that (a) providing the goods or services is not conditioned on the consumer signing the form, (b) the consumer has a right to revoke his or her consent at any time and a description of how he or she may do so, and (c) any consumer health data sold may be subject to redisclosure by a purchasing person and may no longer be protected by the bill following redisclosure;

5. an expiration date for the consent, which may be up to one year after the consumer signs the form; and

6. the consumer's signature and the date the consumer signs the form.

The required form is not valid if:

1. it has expired;

2. it does not satisfy the bill's requirements above;

3. the consumer has revoked his or her consent;

4. it has been combined with any other document for the purpose of getting consent concerning multiple sales, or offers to sell, consumer health data; or

5. the provision of goods or services is conditioned on the consumer signing the form.

The bill requires each person who gives a form to a consumer to also give them a signed copy of it. It also requires each person who sells or purchases consumer health data to keep a copy of each form for at least six years from when the consumer signed it or the last date it was effective, whichever is later.

Prohibition on Using Geofences (§ 1(c)(1)(B))

Regardless of any other state law, the bill prohibits anyone from implementing a geofence to identify, track, collect data from or send notifications or messages to a consumer that enters the virtual perimeter around a health care provider or health care facility providing health care services on an in-person basis.

Under the bill, a "geofence" is 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 them to establish a virtual boundary that is within 2,000 feet of the perimeter around any physical location. A "health care service" is generally any service provided to any consumer to assess, measure, improve, or learn about the consumer's health.

Restrictions on Processing Consumer Health Data (§ 1(d))

The bill allows a processor to process consumer health data only by a binding contract between the processor and a regulated entity. The contract must provide the processing instructions for and limit the actions which the processor may take with respect to the consumer health data the processor processes on the regulated entity's behalf.

The bill prohibits processors from processing consumer health data in way that is inconsistent with the contract terms. The processor must assist the regulated entity by taking all appropriate and possible technical and organizational measures needed for the regulated entity to do the entity's duties under the bill's consumer health data provisions. If the processor fails to adhere to the regulated entity's processing instructions or processes consumer health data in a manner outside the scope of the contract, the processor is deemed to constitute a regulated entity and is subject to the bill's regulated entity requirements.

Under the bill, "process" and "processing" mean any operation or set of operations done on consumer health data.

§§ 3-6 & 8 — MINORS AND ONLINE SERVICES, PRODUCTS, AND FEATURES

The bill also establishes a framework and sets requirements for how controllers who offer online services, products, and services manage, process, and get consent to use the personal data of "minors" (i.e., those under age 18 who are consumers). Under the bill, "online service, product, or feature" is any service, product, or feature that is provided online, but excludes any (1) telecommunications service, or (2) delivery or use of a physical product. "Controllers," "process," "consent," "personal data," and "consumers" have the same meanings as above (see § 1).

Avoiding Heightened Risk of Harm to Minors (§ 4(a))

If a controller offers an online service, product, or feature to consumers who it has actual knowledge, or willfully disregards, are minors, the bill requires the controller to use reasonable care to avoid having their online service, product, or feature proximately cause any heightened risk of harm to minors.

Under the bill, "heightened risk of harm to minors" is processing minors' personal data, including through using any "algorithm" (i.e., any computerized procedure with a set of steps used to accomplish a predetermined objective), in a way that presents any reasonably

foreseeable risk of any:

1. unfair or deceptive treatment of, or any unlawful disparate impact on, minors;

2. financial, physical, or reputational injury to minors;

3. physical or other intrusion on a minor's solitude, seclusion, private affairs, or concerns, if a reasonable person would be offended by the intrusion; or

4. other substantial injury to minors.

Collecting Minors' Precise Geolocation Data and Processing Minors' Personal Data (§ 4(b))

If a controller offers an online service, product, or feature to consumers who it has actual knowledge, or willfully disregards, are minors, the bill prohibits the controller from collecting minors' precise geolocation data and processing their personal data without first getting the minor's consent or, if the minor is younger than age 13, the minor's parent or legal guardian's consent. A controller that complies with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) is deemed to have satisfied the bill's consent requirement.

The bill also prohibits these controllers from collecting a minor's "precise geolocation data" (see definition in § 1 above) unless (1) the data is needed for the controller to provide the online service, product, or feature and, if so, the controller may only collect the data for the time needed to do that; and (2) the controller gives the minor a signal indicating that it is collecting the data, with the signal being conspicuous to the minor for the entire time.

The bill also prohibits these controllers from processing any minor's personal data:

1. for the purposes of (a) targeted advertising, (b) any sale of personal data, or (c) profiling to further any decision the

controller makes resulting in the controller providing or denying any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services;

2. that is not reasonably necessary to provide the online service, product, or feature;

3. for any processing purpose other than the disclosed purpose at the time the controller collected the personal data;

4. for longer than is reasonably necessary to provide the online service, product, or feature; or

5. in any circumstances in which the minor's personal data is accessible by, or visible to, any other user of the online service, product, or feature.

Under the bill, "targeted advertising" is displaying an advertisement to a minor based on profiling. It does not include an advertisement that is (1) based on the context of a minor's current search query, visit to a website, or online application, or (2) directed to a minor in response to his or her current request for information or feedback. It also excludes processing personal data solely to measure or report advertising frequency, performance, or reach.

"Profiling" is any form of automated processing done 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 (CGS § 42-515(22)).

"Sale of personal data" is the exchange of personal data for monetary or other valuable consideration by the controller to a "third party" (an individual or legal entity other than the consumer or controller or processor or their affiliate). It excludes the following:

1. disclosing personal data (a) to a processor that processes it on the controller's behalf, (b) to a third party for providing a product or service the consumer requested, or (c) where the consumer directs the controller to disclose the data or intentionally uses the controller to interact with a third party;

2. disclosing or transferring personal data to (a) the controller's affiliate or (b) a third party as an asset that is part of an actual or proposed merger, acquisition, bankruptcy, or other transaction where the third party assumes control of all or part of the controller's assets; and

3. disclosing personal data that the consumer (a) intentionally made available to the general public through mass media and (b) did not restrict to a specific audience (CGS § 42-515(26)).

Interface Prohibitions (§ 4(c))

If a controller offers an online service, product, or feature to consumers who it has actual knowledge, or willfully disregards, are minors, the bill also prohibits it from:

1. using any user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, including any practice the Federal Trade Commission refers to as a "dark pattern," to lead or encourage any minor to provide any personal data that is not reasonably necessary to provide the online service, product, or feature;

2. by default, using any system design feature to increase, sustain, or extend any minor's use of the online service, product, or feature by, among other things, automatically playing any media, offering any reward to encourage the minor to spend time using the online service, product, or feature, or sending notifications to the minor;

3. allowing any minor's parent, legal guardian, or any other

consumer to monitor the minor's online activity unless the controller provides the minor a signal, which is obvious to the minor, that he or she is being monitored; or

4. allow any adult to contact any minor through any messaging apparatus unless the adult previously established and maintains an ongoing, lawful relationship with the minor.

Data Protection Assessment (§ 5)

The bill requires each controller that, on or after July 1, 2025, offers any online service, product, or feature to consumers who it has actual knowledge, or willfully disregards, are minors to do a data protection assessment of its online service, product, or feature. The assessment must be done consistently with the requirements in the data protection assessment required under the state's consumer data privacy and online monitoring law (CGS § 42-522, see BACKGROUND). (It is not clear which specific requirements apply to the bill's assessment.)

The assessment must also address:

1. the purpose of the online service, product, or feature;

2. the categories of minors' personal data that the online service, product, or feature processes;

3. the purposes for which the controller processes minors' personal data with respect to the online service, product, or feature; and

4. any heightened risk of harm to minors that is a reasonably foreseeable result of offering the online service, product, or feature to minors.

Under the bill, each controller that does a data protection assessment must: (1) review the assessment at least biennially and (2) maintain documentation on the assessment as long as the controller offers the online service, product, or feature to minors. Additionally, for controllers with assessments that show their online service, product, or feature poses a heightened risk to minor, the bill requires them to make

and implement a plan to mitigate or eliminate the risk before offering the service, product, or feature to consumers who they have actual knowledge, or willfully disregard, are minors.

Processors' Duties and Contracts With Controllers (§ 6)

The bill imposes the same obligations to controllers' processors as under the state's existing consumer data privacy and online monitoring law (CGS § 42-521). This includes adhering to the controller's instructions and helping them meet their obligations under the bill and providing the needed information for controllers to do data protection assessments.

Contract. Under the bill, a contract between a processor and controller must govern the processor's data processing procedures for processing done on the controller's behalf. The contract must be binding and have clear instructions for processing data, the processing's nature, purpose, and duration, and both parties' rights and obligations.

The contract must also require the processor to do the following:

1. ensure that each person processing personal data is subject to a duty of confidentiality regarding the data;

2. at the controller's direction, delete or return all personal data to the controller as requested at the end of providing services unless the law requires that it be kept;

3. upon the controller's reasonable request, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations under the bill;

4. after giving the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the processor's obligations on personal data; and

5. either (a) allow, and cooperate with, the controller or the

controller's designated assessor to make reasonable assessments or (b) arrange for a qualified and independent assessor to do so, as described below.

Under the bill, the independent assessor must evaluate the processor's policies and technical and organizational measures regarding the bill's requirements, using an appropriate and accepted control standard or framework and assessment procedure for these assessments. The processor must give a report of the assessment to the controller on request.

The bill specifies that these requirements should not be construed as relieving a controller or a processor from liability based on its role in the processing relationship.

Fact-Based Determination for Controller. Under the bill, determining whether a person is acting as a controller or processor for a specific data process is a fact-based determination that depends on the context in which the data is processed. A person that is not limited in processing personal data under a controller's instructions, or that fails to adhere to these instructions, is a controller and not a processor for that specific data processing. A processor that continues to adhere to a controller's instructions with a specific data processing remains a processor. If a processor begins, alone or with others, determining the purposes and means of the personal data processing, the processor is a controller for that processing and may be subject to the bill's enforcement actions.

Violations (§ 8)

From July 1, 2025, to December 31, 2027, the bill allows the attorney general, before initiating any enforcement action or disclosing an alleged violation of the bill's online services provisions, to issue, on a form he prescribes, a written notice of violation to a controller or processor to give it an opportunity to cure the violation.

Within 30 days of getting this notice, the controller or processor may send notice, on a form the attorney general prescribes, to the attorney

general disclosing that it has (1) determined that the controller or processor did not commit the alleged violation or (2) cured the violation and taken sufficient measures to prevent further violations. If the attorney general receives a responding notice and determines that the controller or processor did not commit the alleged violation or has cured it and taken measures to prevent further violations, then the controller or processor will not be liable for any CUTPA civil penalties.

Under the bill, by February 1, 2027, the attorney general must submit a report to the General Law Committee disclosing:

1. the number of notices of violations he issued,
2. the nature of each violation,
3. the number of violations cured within the 30-day period, and
4. any other matters he deems relevant.

Beginning on January 1, 2027, the attorney general may, in determining whether to give a controller or processor the opportunity to cure an alleged violation, consider:

1. the number of violations,
2. the controller's or processor's size and complexity and the nature and extent of their processing activities,
3. the substantial likelihood of injury to the public,
4. the safety of individuals or property, and
5. whether the alleged violation was likely caused by human or technical error.

§ 7 — EXEMPTIONS AND CONSTRUCTION OF CONTROLLERS' AND PROCESSORS' DUTIES

Exemptions

As under the state's existing consumer data privacy and online

monitoring law (CGS § 42-517), the bill's provisions on consumer health data and online services do not apply to certain entities. This includes the following:

1. state bodies, authorities, boards, bureaus, commissions, districts, or agencies or those of its political subdivisions;
2. federally tax-exempt nonprofit organizations;
3. national securities associations registered under federal law;
4. financial institutions or data subject to certain provisions of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); or
5. covered entities or business associates, as defined in HIPAA regulations (e.g., health plans, health care clearinghouses, and health care providers).

The bill also exempts:

1. entities licensed or accredited to offer one or more programs of higher learning that lead to at least one degree; and
2. any air carrier (i.e., a U.S. citizen that provides air transportation by any means) that is regulated under the Federal Aviation Act of 1958 (49 U.S.C. § 40101 et seq.), and the Airline Deregulation Act (49 U.S.C. § 41713).

As under the consumer data privacy and online monitoring law, the bill also exempts certain information and data. Specifically, the following:

1. protected health information under HIPAA (42 U.S.C. § 1320d et seq.);
2. patient identifying information under a federal law on substance use disorder treatment (42 U.S.C. § 290dd-2);
3. identifiable private information under the federal policy for

protecting human subjects (45 C.F.R. Part 46);

4. identifiable private information collected as part of human subject research under the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

5. information and data related to protecting human subjects (21 C.F.R. Parts 6, 50 and 56) or personal data used or shared in research done following the standards for protecting human subjects the bill exempts above, or other research done following applicable law (45 C.F.R. § 164.501);

6. information and documents created for the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. § 11101 et seq.);

7. patient safety work product for patient safety organizations under state law (CGS § 19a-127o) and the federal Patient Safety and Quality Improvement Act (42 U.S.C. § 299b-21 et seq.);

8. information derived from any health care related information listed in the information or data exemption list that is de-identified according to HIPAA's de-identification requirements;

9. information originating from and intermingled to be indistinguishable with, or treated in the same way as, other exempt information under the bill maintained by a covered entity (e.g., health care providers and plans) or business associate, program, or qualified service organization, as specified in a federal law on substance use disorder treatment (42 U.S.C. § 290dd-2);

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 relating to 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 activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

12. personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

13. personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g et seq.);

14. personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.);

15. data processed or maintained (a) in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role; (b) as an individual's emergency contact information and used for emergency contact purposes; or (c) that must be retained to administer benefits for another individual whose data is HIPAA-protected; and

16. personal data collected, processed, sold, or disclosed in relation to price, route, or service, as used in the federal Airline Deregulation Act (49 U.S.C. § 40101 et seq.), by an air carrier subject to that bill, to the extent this bill is preempted by the Airline Deregulation Act (49 U.S.C. § 41713).

Ability to Collect, Use, or Retain Data

As under the consumer data privacy and online monitoring law (CGS § 42-524), the bill also specifies that the bill's obligations on consumer

health data and online services that it imposes on controllers and processors do not restrict their ability to collect, use, or retain data for internal use to:

1. do internal research to develop, improve, or repair products, services, or technology;

2. recall products;

3. identify and repair technical errors that impair existing or intended functionality; or

4. perform internal operations that are reasonably aligned with the minor's expectations, reasonably anticipated based on the minor's existing relationship with the controller, or compatible with processing data based on providing a product or service the minor specifically requested.

Evidentiary Privilege

The bill's obligations on consumer health data and online services that it imposes on controllers or processors do not apply if doing so would make them violate state evidentiary privilege. The bill should not be construed to prevent a controller or processor from giving personal data about a minor to a person covered by state evidentiary privilege laws as a privileged communication.

First Amendment Rights

The bill states that its provisions on consumer health data and online services are not to be construed to impose an obligation on a controller or processor that adversely affects the rights and freedoms of any person, including his or her rights to free speech or freedom of the press guaranteed under the First Amendment of the U.S. Constitution or the state law protecting disclosure of information by news media (CGS § 52-146t). It also does not affect a person processing personal data for a purely personal or household activity.

Limitations on Processing Personal Data

Under the bill, controllers may process personal data to the extent the processing is (1) reasonably necessary and proportionate to the purposes listed above (e.g., for internal research) and (2) adequate, relevant, and limited to what is needed for the specific listed purpose. When applicable, personal data collected, used, or retained must consider the nature and purposes of these actions. The data must be subject to reasonable administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to minors related to its collection, use, or retention.

Under the bill, if a controller or processor processes personal data for a specified purpose through one of the exemptions listed above, the respective controller or processor bears the burden of showing that the processing (1) qualifies for an exemption under the bill and (2) complies with the bill's requirements for processing personal data.

§ 2 — SOCIAL MEDIA PLATFORMS AND MINORS

The bill prohibits social media platforms from establishing an account for a minor under age 16 without a parent's or guardian's consent.

It also requires these platforms to delete a minor's account within 10 days of getting a request from (1) the minor if he or she is age 16 or older but younger than age 18 or (2) the minor's parent or legal guardian if the minor is under age 16. The platform must also, within this timeframe, stop processing the minor's "personal data" (see definition in § 1 above). Relatedly, the bill requires platforms to establish and describe in a privacy notice one or more secure and reliable way of submitting an account deletion request.

Under the bill a "social media platform" is a public or semi-public Internet-based service or application that:

1. is used by a "consumer" (see definition in § 1 above) in Connecticut;

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 the purposes of 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 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.

"Social media platform" does not include a public or semi-public Internet-based service or application that:

1. exclusively provides e-mail or direct messaging services; or

2. primarily consists of news, sports, entertainment, electronic commerce, or content preselected by the provider or for which any chat, comments, or interactive functionality is incidental to, directly related to, or dependent on providing the content.

§ 9 — WARRANT

The bill allows courts to order providers of electronic communications or remote computing services not to disclose the existence of a warrant for a subscriber or customer record to any other person or entity for up to 90 days for certain exigent or security reasons. A court may make this order if it believes the notification will result in:

1. endangering the life or physical safety of an individual;

2. flight from prosecution;

3. destruction of or tampering with evidence;

4. intimidation of potential witnesses; or

5. otherwise seriously jeopardizing the investigation.

Under the bill, an "electronic communication service" is any service that enables its users to send or receive wire or electronic communications. A "remote computing service" involves providing computer storage or processing services to the public by means of an electronic communications system (CGS § 54-47aa and 18 U.S.C. §§ 2510 & 2711).

§§ 10 & 11 — ONLINE DATING OPERATORS

Under the bill, an online dating operator owes a duty of care to any online dating platform user to protect him or her against potential criminal activity of other users. This includes a duty to notify users if the online dating operator has had a communication with another user that the operator determines to have a higher propensity to commit a crime against individuals. (It is unclear what is considered having a higher propensity to commit a crime against individuals or how an operator would make this determination.)

Under the bill, "online dating operators," are defined as anyone who operates a software application (e.g., presumably, an online dating platform) designed to facilitate online dating. An "online dating platform" is a digital service designed to allow users to interact through the Internet to initiate relationships with other individuals for romance, sex, or marriage (i.e., "online dating").

§ 12 — CT ICAC TASK FORCE

The bill statutorily establishes the CT ICAC within the Department of Emergency Services and Public Protection's Division of Scientific Services and requires it to use appropriated money in a way consistent with specific duties in federal law (i.e., 34 U.S.C. § 21114). This federal law requires each state or local task force that is part of the national program to:

1. consist of state and local investigators, prosecutors, forensic specialists, and education specialists dedicated to addressing the task force goals;

2. work consistently toward achieving ICAC purposes;

3. engage in proactive investigations, forensic examinations, and effective prosecutions of Internet crimes against children;

4. provide forensic, preventive, and investigative assistance to parents, educators, prosecutors, law enforcement, and others concerned with Internet crimes against children;

5. develop multijurisdictional, multiagency responses and partnerships to investigate and prosecute Internet crimes against children offenses through ongoing informational, administrative, and technological support to other state and local law enforcement agencies, for these agencies to acquire the needed knowledge, personnel, and specialized equipment;

6. participate in nationally coordinated investigations in any case in which the U.S. attorney general determines participation to be needed, as allowed by the task force's available resources;

7. set or adopt investigative and prosecution standards, consistent with established norms, to which the task force must comply;

8. investigate and seek prosecution on tips related to Internet crimes against children, including tips from Operation Fairplay; the National Internet Crimes Against Children Data System; the National Center for Missing and Exploited Children's CyberTipline; ICAC task forces; and other federal, state, and local agencies; with priority given to investigative leads that indicate the possibility of identifying or rescuing child victims, including those that indicate a likelihood of seriousness of offense or danger to the community;

9. develop procedures for handling seized evidence;

10. maintain (a) the required reports and records under the federal law; and (b) other reports and records as the U.S. attorney general determines; and

11. seek to comply with national standards on the investigation and

prosecution of Internet crimes against children that the U.S. attorney general sets, to the extent the standards are consistent with Connecticut law.

BACKGROUND

Consumer Data Privacy and Monitoring Law

Beginning July 1, 2023, the consumer data privacy and monitoring law sets a framework for controlling and processing personal data. The framework requires a controller to limit the collection of personal data and establish security practices, among other things. It also gives consumers the right to access, correct, delete, and get a copy of their personal data and to opt out of certain types of personal data processing (e.g., targeted advertising) (CGS § 42-515 et seq.).

COMMITTEE ACTION

Judiciary Committee

Joint Favorable Substitute
Yea 24 Nay 13 (03/30/2023)