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)(xii), 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
(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:

<table>
<thead>
<tr>
<th>Section</th>
<th>Effect Date</th>
<th>Amending Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>July 1, 2025</td>
<td>New section</td>
</tr>
<tr>
<td>2</td>
<td>July 1, 2024</td>
<td>New section</td>
</tr>
<tr>
<td>3</td>
<td>July 1, 2025</td>
<td>New section</td>
</tr>
<tr>
<td>4</td>
<td>July 1, 2025</td>
<td>New section</td>
</tr>
<tr>
<td>5</td>
<td>July 1, 2025</td>
<td>New section</td>
</tr>
<tr>
<td>6</td>
<td>July 1, 2025</td>
<td>New section</td>
</tr>
<tr>
<td>7</td>
<td>July 1, 2025</td>
<td>New section</td>
</tr>
<tr>
<td>8</td>
<td>July 1, 2025</td>
<td>New section</td>
</tr>
<tr>
<td>9</td>
<td>October 1, 2023</td>
<td>54-33c</td>
</tr>
<tr>
<td>10</td>
<td>October 1, 2023</td>
<td>21a-435</td>
</tr>
<tr>
<td>11</td>
<td>October 1, 2023</td>
<td>New section</td>
</tr>
<tr>
<td>12</td>
<td>July 1, 2023</td>
<td>29-7b</td>
</tr>
</tbody>
</table>

**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.