General Assembly

January Session, 2021

LCO No. 10099

Amendment

Offered by:
SEN. DUFF, 25th Dist.

To: Subst. Senate Bill No. 893   File No. 360    Cal. No. 222

"AN ACT CONCERNING CONSUMER PRIVACY."

1 Strike everything after the enacting clause and substitute the following in lieu thereof:

"Section 1. (NEW) (Effective from passage) (a) As used in this section and sections 2 to 19, inclusive, of this act, the following words have the following meanings, unless the context clearly requires otherwise:

(1) "Advertisement" means the process by which a person, the advertiser, proposes a commercial transaction or disseminates a public or private communication or message to solicit business or a commercial opportunity.

(2) "Algorithm" means a specific procedure, set of rules or order of operations designed to solve a problem or make a calculation, classification or recommendation.

(3) "Artificial intelligence" means computerized methods and tools, including, but not limited to, machine learning and natural language
processing, that act in a way that resembles human cognitive abilities when it comes to solving problems or performing certain tasks.

(4) "Automated decision system" means any computer program, method, statistical model or process that aims to aid or replace human decision-making using algorithms or artificial intelligence, including analyzing complex datasets about human populations to generate scores, predictions, classifications or recommendations used to make decisions.

(5) "Biometric information" means information that pertains to measurable biological or behavioral characteristics of an individual that can be used singularly or in combination with each other or with other information for automated recognition or identification of a known or unknown individual, including, but not limited to, fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, gait, handwriting, keystroke dynamics and mouse movements. "Biometric information" does not include (A) writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions or physical descriptions such as height, weight, hair color or eye color; (B) donated organs, tissues or parts, or blood, or serum stored on behalf of recipients or potential recipients of living, or cadaveric transplants obtained or stored by a federally designated organ procurement agency, information captured from a patient in a health care setting or information collected, used or stored for health care treatment, payment or operations under the federal Health Insurance Portability and Accountability Act of 1996, or (C) an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

(6) "Browser personal information" means Internet Protocol addresses, system configuration information, Uniform Resource Locators of referring pages, local and language preferences, keystrokes,
and other similar digital sources associated with an individual.

(7) "Collect" means to collect, buy, rent, gather, obtain, receive, trade for or access any personal information pertaining to an individual by any means, online or offline, including, but not limited to, receiving information from the individual or a third party, actively or passively, or obtaining information by observing the individual's behavior.

(8) "Conduct business in the state" means to produce, solicit or offer for use or sale any information, product or service in a manner that intentionally targets or may reasonably be expected to contact individuals.

(9) "Consent" means freely given, specific, informed, unambiguous, opt-in consent by individuals.

(10) "Commission" means the Connecticut Information Privacy Commission established by section 12 of this act.

(11) "Covered entity" means an entity that conducts business in the state, processes personal information by itself or by contracting with a data processor, and (A) has earned or received ten million dollars or more of annual revenue through three hundred transactions or more, or (B) processes or maintains the personal information of ten thousand or more unique individuals during the course of a calendar year.

(12) "Covered interaction" means an interaction between an individual or its household and a covered entity when such covered entity makes available information, products or services to the individual and collects or otherwise processes personal information pertaining to that individual. "Covered interaction" includes, but is not limited to, posting information, offering a product or service, the placement of targeted advertisements, setting up an account or offering membership or other ongoing relationship with a covered entity.

(13) "Data processor" means a person or entity that processes personal information on behalf of a covered entity.
(14) "De-identified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with or be directly linked to a particular individual or household.

(15) "Device" means a tool that is capable of sending, routing or receiving communications to or from another device and intended for use by a single individual or single household or, if used outside of a home, for use by the general public.

(16) "Disclose" means any action, set of actions or omission in which a covered entity, data processor or a third party makes personal information available to another person, intentionally or unintentionally, including, but not limited to, sharing, publishing, releasing, transferring, disseminating, making available, selling, leasing, providing access to, failing to restrict access to or otherwise communicating orally, in writing, electronically or by any other means.

(17) "Entity" means a corporation, partnership, limited partnership, limited liability partnership, limited liability company, single member limited liability company, sole proprietorship or nonstock corporation, but does not include governmental entities.

(18) "Harm" means potential or realized adverse consequences for an individual or society, including, but not limited to:

(A) Direct or indirect financial harm;

(B) Physical harm or threats to individuals or property, including, but not limited to, bias-related crimes and threats, harassment and sexual harassment;

(C) Discrimination in products, services or economic opportunities such as housing, employment, credit, insurance, education or health care on the basis of an individual or class of individuals belonging to, or being perceived as belonging to, one of the protected classes, as defined in section 46a-64c of the general statutes, except as specifically authorized by law;
(D) Interference with or surveillance of First Amendment-protected activities by state actors, except as specifically authorized by law;

(E) Interference with the right to vote or with free and fair elections;

(F) Violation of individuals' rights to due process or equal protection under the law;

(G) Loss of individual control over personal information via nonconsensual sharing of sensitive personal information, data breach, or other actions that violate this section or sections 1 to 18, inclusive, of this act;

(H) The nonconsensual capture of information or communications within an individual's home or where an individual is entitled to have a reasonable expectation of privacy or access control; and

(I) Other effects on an individual that may not be reasonably foreseeable to, contemplated by or expected by the individual to whom the personal information relates, which are nevertheless reasonably foreseeable to, contemplated by or expected by the covered entity, that alter or limit that individual's choices or predetermine results.

(19) "Individual" means a natural person who is a resident of the state.

(20) "Legal request" means any request for personal information issued by a court of competent jurisdiction pursuant to state or federal laws such as subpoenas, court orders, search warrants, pen register and trap and trace orders or wiretap orders.

(21) "Location information" means information pertaining to where an individual has physically been or directly or indirectly reveals an individual's physical location or the location of a device associated with that individual. "Location information" includes, but is not limited to:

(A) Internet protocol addresses;

(B) GPS coordinates;
(C) Cellular phone site location information;

(D) Time-stamped video or other surveillance information that identifies an individual as being in a certain place;

(E) Information derived from transportation cards; and

(F) Information related to an individual's visit to certain locations.

(22) "Governmental entity" means any agency, executive office, department, board, commission, bureau, division or authority of the state, or of any political subdivision thereof.

(23) "Monetize" or "monetization" means to sell, rent, release, disclose, disseminate, trade, make available, transfer or otherwise communicate orally, in writing, or by electronic or other means, an individual's personal information by a covered entity, a third party or a data processor in exchange for monetary or other consideration, as well as to leverage or use an individual's personal information to place a targeted advertisement or to otherwise profit, regardless of whether the individual's personal information changes hands.

(24) "Person" means any natural or legal person.

(25) "Personal information" means information about an individual directly or indirectly captured in a covered interaction, including any information so captured that directly or indirectly identifies, relates to, describes, is capable of being associated with or could reasonably be linked to a particular individual, household or device. Personal information is reasonably linkable to an individual, household or device if used on its own or in combination with other reasonably available information to identify an individual, household or device, regardless of whether the covered entity holds such additional information. "Personal information" includes, but is not limited to, the following information:

(A) First names, middle names, last names, aliases and social media and Internet web site-used usernames;
(B) Government-issued identification and vehicle license plate numbers;

(C) Telephone numbers, including cellular phone numbers, and physical and digital addresses such as Internet protocol addresses and electronic mail addresses;

(D) Date of birth, age, gender, race, ethnicity, national origin and sexual orientation;

(E) Information revealing political opinions or religious or philosophical beliefs held by identified individuals;

(F) Technical identifiers such as a service identification number that can be linked back to an individual;

(G) Biometric information;

(H) Location information;

(I) Medical and health information including an individual’s medical history and search queries related to medical conditions;

(J) Financial data, including Social Security number, details of financial and commercial transactions and credit scores related to the financial capacity of an individual;

(K) Professional data, including resume, job history and other similar records related to an individual;

(L) Information pertaining to an individual’s behavior online, such as a record of the Internet web sites the individual visits or the files the individual downloads;

(M) Browser personal information;

(N) Information pertaining to an individual’s sex life; and

(O) Electronic communications such as messaging, electronic mail
and voice conversations;

(26) "Processing" or "process" means any action or set of actions performed on or with personal information, including, but not limited to, collecting, accessing, using, storing, retaining, sharing, monetizing, analyzing, creating, generating, aggregating, altering, correlating, operating on, decision-making, recording, modifying, organizing, structuring, disclosing, transmitting, selling, licensing, disposing of, destroying, de-identifying or another handling of personal information, including using personal information in automated decision systems.

(27) "Reasonably understandable" means of length and complexity such that an individual with an eighth-grade reading level, as established by the Department of Education, can read and comprehend.

(28) "Sensitive personal information" means the following personal information related to an identified individual:

(A) Race, ethnicity, national origin and sexual orientation;

(B) Date of birth;

(C) Cellular phone number;

(D) Information revealing political opinions or religious or philosophical beliefs held by identified individuals;

(E) Biometric information;

(F) Location information;

(G) Medical and health information, including an individual's medical history and search queries related to medical conditions;

(H) Information pertaining to an individual's sex life;

(I) Social Security number; and

(J) Credit scores related to the financial capacity of an individual.
(29) "Targeted advertisement" means an advertisement directed to an individual or a group of individuals where the advertisement is selected by an automated decision system based on processed personal information obtained or inferred over time from the individual or the groups of individual's devices activities, communications or associations across Internet web sites, applications, services or covered entities. "Targeted advertisement" does not include advertisements directed to an individual solely based upon the individual's current visit to an Internet web site, application, service, covered entity or a direct response to the individual's request for information or feedback.

(30) "Third party" means, with respect to an individual's personal information, any person or governmental entity that is not the covered entity or a data processor.

(31) "Use model" means a discrete purpose for which collected personal information is to be processed, including, but not limited to, first-party marketing, third-party marketing, first-party research and development, third-party research and development and product improvement and development.

Sec. 2. (NEW) (Effective July 1, 2022) (a) The provisions of sections 1 to 18, inclusive, of this act and any regulations adopted pursuant to said sections shall be interpreted and administered in accordance with the following general principles:

(1) Covered entities and data processors shall process personal information and use automated decision systems discreetly and honestly, and only to the extent necessary for carrying out their purpose; and

(2) Covered entities and data processors shall be protective of personal information, loyal to the individuals whose personal information is processed and honest about the risk of processing practices, including the use of automated decision systems.

(b) Covered entities and data processors shall:
(1) Reasonably secure individual personal information from unauthorized access; and

(2) Promptly comply with section 36a-701b of the general statutes in case of a breach of security, as defined in said section.

(c) Covered entities and data processors shall not use personal information, or information derived from personal information, in any way that:

(1) Benefits themselves to the detriment of an individual;

(2) Results in reasonably foreseeable and material physical or financial harm to an individual; or

(3) Would be unexpected and highly offensive to a reasonable individual that provided consent in accordance with sections 1 to 18, inclusive, of this act.

(d) Covered entities and data processors:

(1) Shall not disclose or sell personal information to, or share personal information with, any other person except as consistent with the provisions set forth in sections 1 to 18, inclusive, of this act and any regulations adopted to implement said sections;

(2) Shall not disclose or sell personal information to, or share personal information with, any third party unless that third party enters into a contract with the covered entity that imposes on the third party the same duties of care, loyalty and confidentiality toward the applicable individual as are imposed on the covered entity under sections 1 to 18, inclusive, of this act; and

(3) Shall take reasonable steps to ensure that the practices of any third party to whom the covered entity discloses or sells, or with whom the covered entity shares personal information fulfill the duties of care, loyalty and confidentiality assumed by the third party under the contract described in subdivision (2) of this subsection.
(4) Covered entities shall regularly audit the data security and data
information practices of any such third party and make such audit
publicly available.

Sec. 3. (NEW) (Effective July 1, 2022) (a) Individuals shall have the
right to:

(1) Access all their personal information that was processed by the
covered entity or a data processor;

(2) Access all the information pertaining to the collection and
processing of the individual's personal information, including, but not
limited to:

(A) Where or from whom the covered entity obtained personal
information, from the individual or a third party, whether online or
offline;

(B) The types of third parties to which the covered entity has
disclosed or will disclose captured personal information;

(C) The purposes of the processing;

(D) The categories of personal information concerned;

(E) The names of third parties to which the covered entity had
disclosed the personal information and a log showing when such
disclosure happened; and

(F) The period of retention of the personal information.

(3) Obtain such individual's personal information processed by a
covered entity in a structured, readily usable, portable, and machine-
readable format;

(4) Transmit or cause the covered entity to transmit the personal
information to another covered entity, where technically feasible;

(5) Request a covered entity to stop collecting and processing their
(6) Correct inaccurate personal information stored by covered entities; and

(7) Delete all their personal information stored by covered entities, provided that a covered entity that has collected personal information from an individual is not required to delete information to the extent it is exempt under sections 1 to 18, inclusive, of this act from the requirement of consent.

(b) A covered entity that maintains an individual's personal information in a nonpublic profile or account shall correct or delete such personal information, and any information derived therefrom, pertaining to the individual upon the individual's request.

(c) A covered entity shall provide individuals with a reasonable means to exercise their rights specified in subsection (a) of this section in a form that is:

(1) Clear and conspicuous;

(2) Made available at no additional cost and with no transactional penalty to the individual to whom the information pertains; and

(3) In English and any other language in which the covered entity communicates with the individual to whom the information pertains.

(d) A covered entity shall comply with a request to exercise the rights specified in subsection (a) of this section not later than thirty days after receiving a verifiable request from the individual. Where the covered entity has reasonable doubts or cannot verify the identity of the individual making a request, the covered entity may request additional personal information necessary for the specific purpose of confirming the identity of the individual. A covered entity may not de-identify an individual's personal information during the sixty-day period beginning on the date on which the covered entity receives a request for correction or deletion from the individual.
Sec. 4. (NEW) (Effective July 1, 2022) (a) Individuals shall have the right to know what personal information a covered entity or a data processor will collect and process about the individual, including the categories and specific pieces of personal information the covered entity processes, before giving consent for the collection and processing of their personal information.

(b) A covered entity shall make both a long-form privacy policy and a short-form privacy policy available to all individuals in accordance with the following:

(1) (A) The privacy policies shall be available and readily accessible on the covered entity's Internet web site or mobile application, or

(B) In the case of in-person or non-Internet electronic engagement, the privacy policies shall be readily accessible at the primary physical place of business and any offline equivalent maintained by the covered entity.

(2) The privacy policies shall be persistently and conspicuously available at or prior to the point of sale of a product or service, subscription to a service, sign up or creation of an account with the covered entity.

(3) (A) Covered entities that process personal information shall ensure that individuals are presented with the short-form privacy policy only once upon the individual's first electronic covered interaction that may or will result in the processing of personal information, whether that is through the covered entity's Internet web site or use of the covered entity's mobile application; or

(B) In the case of in-person or non-Internet electronic engagement, the short-form privacy policy should be read to or otherwise presented to the individual before the covered entity first collects the individual's personal information.

(4) The short-form privacy notice required under this section shall (A) be clear, concise, well-organized and complete; (B) be clear and
prominent in appearance; (C) use clear and plain language; (D) use visualizations where appropriate to make complex information understandable by the ordinary user; (E) be reasonably understandable; (F) be distinguishable from other matters; (G) not contain any unrelated, confusing or contradictory information; (H) be no more than six hundred words, excluding the list of third parties with which the covered entity discloses personal information; and (I) be provided free of charge.

(5) The short-form privacy notice required under this section shall include (A) the sensitive personal information being processed; (B) the use model and a brief explanation of the relationship between the individual and the covered entity; (C) whether the covered entity by itself or a data processor on its behalf processes the information; (D) whether the covered entity uses automated decision systems; (E) whether personal information is going to be processed for purposes of targeted advertisement or monetization; (F) an example of harm that may arise from a misuse of the personal information; (G) the period of retention of the personal information expressed in exact dates; (H) to what types of third parties the covered entity discloses personal information and for what purposes, including governmental entities; and (I) whether the covered entity collects personal information through offline practices when the individual does not interact directly with the covered entity.

(6) A list of the third parties referenced in subparagraph (H) of subdivision (5) of this subsection shall be provided either in the short-form privacy notice or in an easily accessible online form. If the policy is delivered verbally, the person communicating the policy shall offer to read the list of third parties. If provided in the short-form privacy notice, such list must be offset by at least two line breaks from the rest of the short-form privacy notice.

(7) The long-form privacy policy shall contain a detailed description of the processing of the personal information, including, but not limited to, all the elements of the short-form privacy policy and an explanation
of how the covered entities and their affiliate data processors comply
with the provisions of sections 1 to 18, inclusive, of this act, including
(A) a brief explanation of the technology that mediates the relationship
between the individual and the covered entity, including automated
decision systems; and (B) a brief explanation of the risks of harm that
arises from the possible misuse of personal information processing.

(c) The commission shall (1) establish a standardized short-form
privacy notice that complies with this section, (2) determine whether a
more concise presentation of a short-form privacy notice is appropriate
where the policy is being communicated verbally, and if so, shall
establish a standardized short-form verbal privacy notice, (3) develop a
recognizable and uniform logo or button to promote individual
awareness of the short-form privacy notice, and (4) adopt regulations in
accordance with the provisions of chapter 54 of the general statutes
specifying additional requirements for the format and substance of
short-form privacy notices.

Sec. 5. (NEW) (Effective July 1, 2022) (a) Individuals shall have the
right to consent in accordance with this section before their personal
information is collected and processed.

(b) Consent given by an individual authorizes a covered entity to
collect, cause to collect, process or cause to process personal information
from such individual in accordance with the following:

(1) A covered entity shall obtain consent (A) before collecting or
causing to collect personal information for purposes of processing an
individual's personal information for the first time; and (B) after the
acceptance of the short-form privacy policy described in section 4 of this
act.

(2) For continuing covered interactions, the consent required by this
section shall be renewed annually, and if not so renewed, shall be
deemed to have been withdrawn.

(3) A covered entity shall provide new meaningful notice and obtain
consent from an individual two weeks before changing the nature of the processing of personal information to which the individual previously consented, except if the change in processing is necessary to enable a new functionality requested by the individual, provided that such individual was given notice and provided consent when making such request.

(c) A covered entity requesting consent shall (A) ensure that the option to refuse consent is presented as clearly and prominently as the option to provide consent; (B) provide a mechanism for an individual to withdraw previously given consent at any time; and (C) once a year, provide a notice explaining how the personal information was used, including two examples of such use.

(d) A covered entity requesting consent shall not coerce consent through the use of interfaces that (1) threaten or mandate an individual's compliance; (2) ask questions or provide information in a way individuals cannot reasonably understand; (3) attract the individual's attention away from the individual's current task by exploiting perception, particularly preattentive processing; (4) take advantage of individuals' errors to facilitate the interface designer's goals; (5) deliberately increase work for the individual; (6) interrupt the individual's task flow; (7) use information architectures and navigation mechanisms that guide the individual toward not having a real option to consent; (8) hide desired content or interface elements; (9) limit or omit controls that would facilitate task accomplishment by the individual; (10) present disturbing content to the individual; or (11) generally mislead or deceive the individual.

(e) Once an individual refuses to provide consent in accordance with this section, and if the individual keeps interacting with the covered entity in any way, the covered entity shall not try to obtain consent unless a period of at least six months has passed.

(f) Under no circumstances shall the mere covered interaction of an individual with a covered entity's product or service be deemed as
(g) A covered entity may collect browser personal information, provided that the covered entity (1) processes only the personal information necessary to request consent; (2) processes such information solely to request consent; and (3) immediately deletes all the personal information if consent is refused, except the covered entity shall retain the personal information necessary to comply with subsection (e) of this section, and such information shall only be used to comply with said subsection.

(h) (1) Except as provided in subdivision (2) of this subsection, a covered entity shall not (A) refuse to serve an individual who does not approve the processing of the individual's personal information under this section unless the processing is necessary for the primary purpose of the transaction that the individual has requested; or (B) offer a program that relates the price or quality of a product or service to the degree of acceptance of personal information processing, including the provision of discounts or other incentives in exchange for the consent.

(2) A covered entity may, with the individual's consent given in compliance with this section, operate a program in which information, products, or services sold to the individual are discounted based on that individual's prior purchases from the covered entity, provided that the personal information shall be processed solely to operate such program.

(3) A covered entity shall not state or imply that the quality of a product or service will be diminished and shall not actually diminish the quality of a product or service if the individual declines to give consent.

Sec. 6. (NEW) (Effective July 1, 2022) (a) Individuals shall have the right to (1) know the names of third parties to which the covered entities or data processors will disclose their personal information, and (2) refuse consent for such disclosure.

(b) No covered entity or data processor in possession of personal
information may disclose, cause to disclose or otherwise disseminate to third parties, including government agencies, personal information unless (1) such disclosure is included in the meaningful notice pursuant to section 4 of this act, and (2) consent from the individual is obtained in the manner prescribed in section 5 of this act. Except as provided in subsection (c) of this section, a covered entity shall not process or cause to process an individual's personal information acquired from a third party, unless it has first obtained the individual's consent.

(c) If the processing is necessary to obtain consent, the covered entity shall (A) process only the personal information required to request consent; (B) process the personal information solely to request consent; and (C) immediately delete the personal information if consent is not given.

(d) A covered entity shall not disclose personal information to a data processor or another third party without a contractual agreement that (A) requires the data processor or third party to meet the same privacy and security obligations as the covered entity; (B) prohibits the data processor or third party from processing the personal information for any purpose other than the purposes for which the individual provided consent; and (C) prohibits the data processor or third party from further disclosing or processing the personal information except as explicitly authorized by the contract and consistent with sections 1 to 18, inclusive, of this act.

(e) If a covered entity learns that a data processor or third party to whom it has provided access to personal information is using such personal information in violation of sections 1 to 18, inclusive, of this act, the covered entity shall immediately (A) limit the violator's access to personal information; (B) seek proof of destruction of personal information previously accessed by the violating data processor or third party; and (C) notify the commission about the violation.

Sec. 7. (NEW) (Effective July 1, 2022) (a) A covered entity shall not activate the microphone, camera or any other sensor on a device in the
lawful possession of an individual that is capable of collecting or
transmitting audio, video or image data or data that can be used to
measure biological or biometric information, human movement,
location, chemicals, light, radiation, air pressure, speed, weight or mass,
positional or physical orientation, magnetic fields, temperature or
sound without providing notice and obtaining consent pursuant to
sections 1 to 18, inclusive, of this act for the specific type of measurement
to be activated, provided that such consent shall be effective for not
more than one hundred eighty days, after which it shall expire unless
renewed.

Sec. 8. (NEW) (Effective July 1, 2022) (a) For the purposes of sections 1
to 18, inclusive, of this act, individuals age thirteen and older are
deemed competent to exercise all rights granted to individuals under
sections 1 to 18, inclusive, of this act.

(b) Rights and obligations relating to individuals under the age of
thirteen shall be governed by the Children's Online Privacy Protection
Act, 15 USC 6501 et seq., and any regulations adopted pursuant to said
act.

Sec. 9. (NEW) (Effective July 1, 2022) (a) In addition to all provisions of
sections 1 to 18, inclusive, of this act generally applicable to personal
information, the following provisions shall apply to the processing and
collection of biometric and location information, regardless of how such
biometric and location information is processed or collected:

(1) No covered entity or data processor may collect or process an
individual’s biometric or location information unless it first (A) informs
the individual in writing that biometric or location information is being
processed and the specific purpose or purposes and length of time for
which the information is being processed; and (B) obtains consent from
the individual for the specific purpose of collecting and processing
biometric or location information before any such information is
collected or processed.

(2) For biometric information, the consent shall be handwritten and
executed by the individual, explicitly authorize such processing, and be sent to the covered entity by postal mail, facsimile, or electronic scan.

(3) Consent shall be for a period specified in the written consent of not more than one year and shall automatically expire at the end of such period unless renewed pursuant to the same procedures. Upon expiration of consent, any biometric or location information possessed by a covered entity shall be destroyed.

(4) A covered entity in possession of biometric or location information shall develop a specific written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric or location information when the initial purpose for processing such information has been satisfied or within one year of the individual’s consent, unless renewed, whichever occurs first.

(5) Absent a valid warrant issued by a court of competent jurisdiction, a covered entity in possession of biometric or location information shall comply with its established retention schedule and destruction guidelines.

(6) No covered entity or data processor in possession of biometric or location information may disclose, cause to disclose, sell or otherwise disseminate or cause to disseminate to third parties, including government agencies, an individual’s biometric or location information unless (A) the individual gives consent in writing to the disclosure; (B) the disclosure completes a financial transaction requested or authorized by the subject of the biometric or location information; (C) the disclosure is required by state or federal law, in which case the individual shall be given adequate notice on the occasion of obtaining the consent; or (D) the disclosure is required pursuant to a valid warrant issued by a court of competent jurisdiction, in which case the individual shall be given adequate notice in accordance with section 16 of this act.

(7) Except as provided in subsection (b) of this section, no covered entity in possession of biometric or location information may monetize
or otherwise profit from an individual's biometric or location information.

(b) A covered entity may process an individual's biometric or location information to recommend actions, services, goods or products provided (1) there is full disclosure to the individual about the biometric or location information processed; (2) consent was given in a manner consistent with this section; and (3) there is full disclosure that such recommendation is based on the biometric or location information processed.

Sec. 10. (NEW) (Effective July 1, 2022) (a) Individuals shall have the right not to be subject to processing of their personal information that results in unlawful discriminatory actions.

(b) Covered entities that process personal information shall not engage in unlawful discriminatory practices connected with the use of personal information and the provision of services, products or goods.

(c) Unlawful discriminatory practices are acts or practices that:

(1) Process personal information in the course of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting or otherwise commercially contracting for employment, finance, health care, credit, insurance, housing or education opportunities in a manner that directly results in discrimination against or otherwise makes an opportunity unavailable on the basis of an individual's or group of individuals' actual or perceived belonging to a protected class, as defined in section 46a-64c of the general statutes;

(2) Process personal information in a manner that discriminates in, or otherwise makes unavailable, whether in a commercial transaction or otherwise, any place of public accommodation, resort or amusement as set forth in chapter 814c of the general statutes, on the basis of an individual's or group of individuals' actual or perceived belonging to a protected class, as defined in section 46a-64c of the general statutes; or
(3) Enable the use of covered entities' services or products to place targeted advertisements for employment, finance, health care, credit, insurance, housing or education opportunities in such a way that enables the advertiser to determine whether to serve an advertisement to an individual or group of individuals on the basis of actual or perceived belonging to a protected class, as defined in section 46a-64c of the general statutes.

(d) Nothing in this section shall limit covered entities from processing personal information for (1) legitimate testing to prevent unlawful discrimination or otherwise determine the extent or effectiveness of the covered entity's compliance with this section; and (2) the purpose of advertising, marketing, soliciting or offering education or employment opportunities to members of a protected class, as defined in section 46a-64c of the general statutes so long as such opportunities are within an affirmative action, diversity program or similar initiative that intends to provide opportunities to the protected classes.

Sec. 11. (NEW) (Effective January 1, 2023) (a) Covered entities that process personal information shall be in violation of sections 1 to 18, inclusive, of this act in connection with the use of personal information and the provision of services, products or goods if their acts or practices (1) materially interfere with the ability of an individual to understand the way the covered entity processes personal information; or (2) take unreasonable advantage of (A) a lack of understanding on the part of the individual of the material risks, costs or conditions of the processing of personal information; (B) the inability of the individual to protect the interests of the individual in selecting or using a product, good or service provided by the covered entity; or (C) the reasonable reliance by the individual on a covered entity to act in the interests of the consumer.

(b) A violation of the requirements of section 1 to 18, inclusive, of this act shall constitute an unfair trade practice for purposes of section 42-110b of the general statutes and shall be enforced by the Attorney General and may be subject to a right of action under section 42-110g of the general statutes.
Sec. 12. (NEW) (Effective from passage) (a) There is established a Connecticut Information Privacy Commission, which shall be part of the Executive Department.

(b) The commission shall consist of the following members: (1) One appointed by the speaker of the House of Representatives; (2) one appointed by the president pro tempore of the Senate; (3) one appointed by the majority leader of the House of Representatives; (4) one appointed by the majority leader of the Senate; (5) one appointed by the minority leader of the House of Representatives; (6) one appointed by the minority leader of the Senate; (7) the Commissioner of Consumer Protection, or the commissioner's designee; and (8) a representative of the Office of the Attorney General.

(c) All initial appointments to the commission shall be made not later than sixty days after the effective date of this section. The Governor shall select the chairpersons of the commission from among the members of the commission. Such chairpersons shall schedule the first meeting of the commission, which shall be held not later than sixty days after the effective date of this section.

(d) Appointed members of the commission shall serve for four-year terms which shall commence on the date of appointment. Members shall continue to serve until their successors are appointed. Any vacancy shall be filled by the appointing authority. Any vacancy occurring other than by expiration of term shall be filled for the balance of the unexpired term.

(e) A majority of the commission shall constitute a quorum for the transaction of any business.

(f) The members of the commission shall serve without compensation, but shall, within the limits of available funds, be reimbursed for expenses necessarily incurred in the performance of their duties.

(g) The commission shall appoint an executive director. The executive
director shall serve at the pleasure of the commission, shall receive such
salary as may be determined by the commission and shall devote full
time and attention to the duties of the office. The executive director shall
be a person with skill and experience in management, and shall be the
executive and administrative head of the commission. The executive
director shall appoint and employ a chief financial and accounting
officer and may, subject to the approval of the commission, employ
other employees, consultants, agents and advisors, including legal
counsel, and shall attend meetings of the commission. The chief
financial and accounting officer of the commission shall be in charge of
its funds, books of account and accounting records. No funds shall be
transferred by the commission without the approval of the commission
and the signatures of the chief financial and accounting officer and the
treasurer of the commission. In the case of an absence or vacancy in the
office of the executive director or in the case of disability, as determined
by the commission, the commission may designate an acting executive
director to serve as executive director until the vacancy is filled or the
absence or disability ceases. The acting executive director shall have all
of the powers and duties of the executive director and shall have similar
qualifications as the executive director.

(h) The commission shall have the following powers and duties: (1)
On and after January 1, 2023, to investigate and enforce violations of
sections 1 to 18, inclusive, of this act; (2) to obtain from any executive
department, board, commission or other agency of the state such
assistance and data as necessary and available to carry out the purposes
of this section; (3) to accept any gift, donation or bequest for the purpose
of performing the duties described in this section; (4) to create and
disseminate information to the public about their rights in relation to
personal information privacy and what to do if they believe their rights
have been violated; and (5) to perform such other acts as may be
necessary and appropriate to carry out the duties described in this
section.

(i) Not later than February 1, 2022, and annually thereafter, the
commission shall submit a report, in accordance with the provisions of
section 11-4a of the general statutes, to the Governor and the joint standing committee of the General Assembly having cognizance of matters relating to general law that shall include, but need not be limited to: (1) The activities of the commission during the prior year; and (2) recommendations for policy changes and amendments to the general statutes necessary to implement the provisions of sections 1 to 18, inclusive, of this act.

(j) The commission shall, subject to the provisions of chapter 67 of the general statutes, employ such employees as may be necessary to carry out the provisions of this section. The commission may enter into such contractual agreements as may be necessary for the discharge of its duties, within the limits of its appropriated funds and in accordance with established procedures.

(k) The commission may (1) make investigations on its own initiative or upon written complaint under oath by any individual, with respect to alleged violations of any provision of sections 1 to 18, inclusive, of this act, (2) hold hearings when the commission deems necessary to investigate such violations, (3) for the purpose of such hearings, administer oaths, examine witnesses and receive oral and documentary evidence, and (4) subpoena witnesses under procedural rules the commission shall adopt, to compel their attendance and to require the production for examination of any books and papers which the commission deems relevant to any matter under investigation or in question. Until the commission determines that it is necessary to investigate a violation, commission members and staff shall keep confidential any information concerning a complaint or preliminary investigation, except upon request of the entity that is the subject of the complaint or preliminary investigation. In case of a refusal to comply with any subpoena issued pursuant to this subsection or to testify with respect to any matter upon which that person may be lawfully interrogated, the superior court for the judicial district of Hartford, on application of the commission, may issue an order requiring such person to comply with such subpoena and to testify; failure to obey any such order of the court may be punished by the court as a contempt
thereof. The commission, after reviewing and investigating any alleged
violation of sections 1 to 18, inclusive, of this act, may impose a civil
penalty and shall report to the office of the Attorney General any such
violation along with the commission's findings concerning such
violation. The commission may refer cases for criminal prosecution to
the appropriate federal, state or local authorities.

(l) The commission shall adopt regulations in accordance with the
provisions of chapter 54 of the general statutes to implement the
provisions of sections 1 to 18, inclusive, of this act.

Sec. 13. (NEW) (Effective January 1, 2023) (a) Any individual or group
of individuals alleging a violation of sections 1 to 18, inclusive, of this
act or a regulation promulgated under said sections may bring an
administrative complaint before the commission. The commission shall
create a form of complaint for use under this section, which shall be in
such form and language to permit an individual to prepare and file such
complaint pro se. An individual shall not be required to accept
mandatory arbitration of a claim under sections 1 to 18, inclusive, of this
act as a condition of bringing an administrative complaint. The
administrative complaint shall be directed against the covered entity,
data processor and the third parties alleged to have committed the
violation. The commission shall investigate the allegations and decide
whether it amounts to the imposition of a civil administrative penalty.

(b) The commission shall also open investigations without any
particular alleged violation to assess the compliance of covered entities,
data processors and third parties with sections 1 to 18, inclusive, of this
act and shall impose civil administrative penalties if necessary.

(c) Whenever the commission seeks to assess a civil administrative
penalty on any covered entities, data processors and third parties, the
commission shall cause to be served upon such person, either by service,
in hand or by certified mail, return receipt requested, a written notice of
its intent to assess a civil administrative penalty that shall include a
concise statement of the alleged act or omission for which such civil
administrative penalty is sought to be assessed, each law, regulation or
order violated as a result of such alleged act or omission; the amount the
commission seeks to assess as a civil administrative penalty for each
such alleged act or omission; a statement of such person's right to an
adjudicatory hearing in accordance with the provisions of chapter 54 of
the general statutes on the proposed assessment; the requirements such
person shall comply with to avoid being deemed to have waived the
right to an adjudicatory hearing; and the manner of payment thereof if
such person elects to pay the penalty and waive an adjudicatory
hearing. After such notice of intent to assess a civil administrative
penalty has been given, each such day thereafter during which such
noncompliance or violation occurs or continues shall constitute a
separate offense and shall be subject to a separate civil administrative
penalty if reasonable efforts have not been made to promptly come into
compliance.

(d) Whenever the commission seeks to assess a civil administrative
penalty on any person, such person shall have the right to an
adjudicatory hearing under chapter 54 of the general statutes. Such
person shall be deemed to have waived such right to an adjudicatory
hearing unless, within twenty-one days of the date of the commission's
notice of intent to assess a civil administrative penalty, such person files
with the commission a written statement denying the occurrence of any
of the acts or omissions alleged by the commission in such notice, or
asserting that the money amount of the proposed civil administrative
penalty is excessive. In any adjudicatory hearing, the commission shall,
by a preponderance of the evidence, prove the occurrence of each act or
omission alleged by the commission.

(e) If a person waives such person's right to an adjudicatory hearing,
the proposed civil administrative penalty shall be final immediately
upon such waiver.

(f) If a civil administrative penalty is assessed at the conclusion of an
adjudicatory hearing, such civil administrative penalty shall be final
upon the expiration of thirty days if no appeal of such decision is
commenced pursuant to section 4-183 of the general statutes.

(g) Any person who files an appeal under section 4-183 of the general statutes of the final assessment of a civil administrative penalty shall place the full amount of the final assessment in an interest-bearing escrow account in the custody of the clerk of the reviewing court. The establishment of such an interest-bearing escrow account shall be a condition precedent to the jurisdiction of the reviewing court unless the party seeking judicial review demonstrates in a preliminary hearing held within twenty days of the filing of the complaint either the presence of a substantial question for review by the court or an inability to pay. Upon such a demonstration, the court may grant an extension or waiver of the interest-bearing escrow account or may require, in lieu of such interest-bearing escrow account, the posting of a bond payable directly to the state in the amount of one hundred twenty-five per cent of the assessed penalty. If, after judicial review, in a case where the requirement for an escrow account has been waived, and in cases where a bond has been posted in lieu of such requirement, the court affirms, in whole or in part, the assessment of a civil administrative penalty, the commission shall be paid the amount thereof together with interest at twelve per cent. If, after such review in a case where an interest-bearing escrow account has been established, the court affirms the assessment of such penalty, in whole or in part, the commission shall be paid the amount thereof together with the accumulated interest thereon in such interest-bearing escrow account. If the court sets aside the assessment of a civil administrative penalty in a case where the amount of such penalty has been deposited in an interest-bearing escrow account, the person on whom the civil administrative penalty was assessed shall be repaid the amount so set aside, together with the accumulated interest thereon.

(h) Any person who fails to pay a civil administrative penalty on time, and who issues a bond pursuant to this section and who fails to pay to the state on time the amount required under this section, shall be liable to the state for up to three times the amount of the civil administrative penalty, together with costs, plus interest from the time
the civil administrative penalty became final and attorneys' fees, including all costs and attorneys' fees incurred directly in the collection thereof. The rate of interest shall be twelve per cent.

(i) No civil administrative penalty assessed under this section shall be: (1) Less than fifteen-hundredths per cent of the annual global revenue of the covered entity, data processor or third party or fifteen thousand dollars, whichever is greater, per individual violation; or

(2) More than four per cent of the covered entity's annual global revenue, data processor or third party or twenty million dollars, whichever is greater, if the commission assesses a civil administrative penalty for multiple violations that affect multiple individuals.

(j) In determining the amount of each civil administrative penalty, the commission shall include, but not be limited to, the following in its consideration: (1) The number of affected individuals; (2) the severity of the violation or noncompliance; (3) the risks caused by the violation or noncompliance; (4) whether the violation or noncompliance was part of a pattern of violations and noncompliance and not an isolated instance; (5) whether the violation or noncompliance was wilful and not the result of error; (6) the precautions taken by the defendant to prevent a violation; (7) the number of administrative actions, lawsuits, settlements and consent decrees under sections 1 to 18, inclusive, of this act involving the defendant; (8) the number of administrative actions, lawsuits, settlements and consent decrees involving the defendant in other states and at the federal level in issues involving information privacy; and (9) the international record of the defendant when it comes to information privacy issues;

(k) Notwithstanding any provision of the general statutes, including the limitations and considerations set forth in this section, the commission may require that the amount of a civil administrative penalty imposed pursuant to this section exceeds the economic benefit realized by a person for noncompliance.

(l) When imposing civil administrative penalties, the commission
shall consider the following: (1) Each individual whose personal
information was unlawfully processed, and each instance of processing
counts as a separate violation; and (2) if a series of steps or transactions
were component parts of a single transaction to avoid the reach of
sections 1 to 18, inclusive, of this act, the commission shall disregard the
intermediate steps or transactions and consider everything one
transaction.

(m) All civil administrative penalties assessed shall be paid to the
state, to the State Treasurer. Once the payment is received, the state shall
deposit ten per cent of any such penalty in the Connecticut Privacy
Commission account and the remaining proceeds shall be used to
redress and mitigate harms caused by the violation to identified
individuals.

(n) There is established an account to be known as the "Connecticut
Privacy Commission account" which shall be a separate, nonlapsing
account within the General Fund. The account shall contain any moneys
required by law to be deposited in the account. Moneys in the account
shall be expended by the Connecticut Privacy Commission for the
purposes of fulfilling its duties under section 12 of this act.

Sec. 14. (NEW) (Effective July 1, 2022) (a) Any provision of a contract
or agreement of any kind, including a covered entity's terms of service
or a privacy policy, including the short-form privacy notice required
under section 4 of this act that purports to waive or limit in any way an
individual's rights under sections 1 to 18, inclusive, of this act, including,
but not limited to, any right to a remedy or means of enforcement shall
be deemed contrary to public policy and shall be void and
unenforceable.

(b) No covered entity that is a provider of an interactive computer
service, as defined in 47 USC 230, shall be treated as the publisher or
speaker of any personal information provided by another information
content provider, as defined in 47 USC 230 and allowing posting of
information by a user without other action by the interactive computer
service shall not be deemed processing of the personal information by
the interactive computer service.

(c) No private or government action brought pursuant to sections 1
to 18, inclusive, of this act shall preclude any other action under sections
1 to 18, inclusive, of this act.

Sec. 15. (NEW) (Effective July 1, 2022) (a) A covered entity shall not be
required to provide meaningful notice or obtain consent for processing
personal information in accordance with sections 4 and 5 of this act
when:

(1) (A) Except as provided in subparagraph (B) of this subdivision,
the processing is necessary to execute the specific transaction for which
the individual is providing personal information, such as the provision
of financial information to complete a purchase or the provision of a
mailing address to deliver a package;

(B) Personal information shall not be processed for any other purpose
beyond that clear primary purpose without providing meaningful
notice to and obtaining consent from the individual to whom the
personal information pertains;

(2) The covered entity believes that:

(A) An emergency involving immediate danger of death or serious
physical injury to any individual requires obtaining without delay
personal information so that it can be used to respond to the emergency,
and

(B) the request is narrowly tailored to address the emergency, subject
to the following limitations:

(i) The request shall document the factual basis for believing that an
emergency involving immediate danger of death or serious physical
injury to an individual requires obtaining without delay personal
information relating to the emergency; and
Simultaneous with the covered entity obtaining personal information under this paragraph, the covered entity shall use reasonable efforts to inform the individual of the personal information obtained, the details of the emergency and the reasons why the covered entity needed to obtain the personal information and shall continue such efforts to inform until receipt of information is confirmed; or

(3) The processing involves only de-identified information, provided that a covered entity that processes de-identified information shall:

   (A) Have a privacy policy that details how the de-identified information is processed;

   (B) Implement technical safeguards that prohibit indirect re-identification of the information;

   (C) Implement business processes that expressly prohibit indirect re-identification of the information;

   (D) Implement business processes that prevent inadvertent release of de-identified information; and

   (E) Not attempt to re-identify the information.

(b) A covered entity, its affiliated data processors or the third parties they contracted with shall not be required to obtain consent for disclosing or sharing personal information in accordance with sections 1 to 18, inclusive, of this act if disclosure is required to respond to a legal request, provided a covered entity receiving such legal request shall serve or deliver the following information to the individual to which the legal request for personal information refers by registered or first-class mail, electronic mail or other means reasonably calculated to be effective:

   (1) A copy of the legal request and a notice that informs the individual of the nature of the inquiry with reasonable specificity;

   (2) The personal information related to the individual that was
supplied to, or requested by, a requesting entity and the date on which
the supplying or request took place;

(3) An inventory of the personal information requested or supplied;

(4) Whether the information was in possession of the covered entity,
an affiliate data processor or a third party they contracted with; and

(5) The identity of the person that sought the legal request from the
court, if known.

(c) The covered entity shall serve or deliver such notification
immediately upon receiving a legal request asking for or compelling the
disclosure of personal information, provided that a covered entity may
apply to the court for an order delaying notification. The court may issue
the order if notification of the existence of the legal request will result in
danger to the life or physical safety of an individual, flight from
prosecution, destruction of or tampering with evidence or intimidation
of potential witnesses or otherwise seriously jeopardize an investigation
or unduly delay a trial. If granted, such an order shall not exceed thirty
days but may be renewed up to thirty days at a time while grounds for
the delay persist.

(d) A covered entity, its affiliated data processors or the third parties
they contracted with shall not be required to obtain consent for
disclosing or sharing personal information in accordance with sections
1 to 18, inclusive, of this act if disclosure is a routine disclosure required
by state or federal law, provided the individual received notice of such
requirement in accordance with sections 4 and 6 of this act.

Sec. 16. (NEW) (Effective July 1, 2022) (a) Covered entities that receive
any form of a legal request for disclosure of personal information
pursuant to sections 1 to 18, inclusive, of this act shall:

(1) Provide the commission and the general public a bimonthly report
containing the following aggregate information related to legal requests
received by the covered entity, their affiliated data processors and any
third parties they contracted with: (A) The total number of legal
requests, disaggregated by type of requests such as warrants, court
orders and subpoenas; (B) the number of legal requests that resulted in
the covered entity disclosing personal information; (C) the number of
legal requests that did not result in the covered entity disclosing
personal information, including the reasons why the information was
not disclosed; (D) the type of personal information sought in the legal
requests received by the covered entity; (E) the total number of legal
requests seeking the disclosure of location or biometric information; (F)
the number of legal requests that resulted in the covered entity
disclosing location or biometric information; (G) the number of legal
requests that did not result in the covered entity disclosing location or
biometric information, including the reasons for not disclosing such
information; and (H) the nature of the proceedings from which the
requests were ordered and whether it was a governmental entity or a
private person seeking the legal request;

(2) Take all reasonable measures and engage in all legal actions
available to ensure that the legal request is valid under applicable laws
and statutes; and

(3) Require their affiliate data processors and third parties they
contracted with to have similar practices and standards.

(b) Covered entities that are required to disclose personal information
as a matter of law pursuant to subdivision (2) of subsection (b) of section
16 of this act shall provide the commission and the general public a
bimonthly report containing the following aggregate information:

(1) The total number of times that they share information,
disaggregated by: (A) Applicable law that mandates such disclosure; (B)
governmental entity or private party that received the information; and
(C) the type of personal information disclosed.

(2) The total number of individuals affected by such disclosures,
disaggregated by race, ethnicity, gender and age, if such demographics
are known.
(c) The commission shall (1) establish a standardized reporting form to comply with this section, (2) determine whether a more concise presentation of the reporting is appropriate and, if so, shall establish a standardized version of such form, (3) dedicate a section of its Internet web site to making the reports available to the general public, and (4) adopt regulations, in accordance with the provisions of chapter 54 of the general statutes, specifying additional requirements for purposes of advancing information related to the sharing of information with the government.

Sec. 17. (NEW) (Effective July 1, 2022) Sections 1 to 18, inclusive, of this act shall not apply to:

(1) Personal information captured from a patient by a health care provider or health care facility or biometric information collected, processed, used or stored exclusively for medical education or research, public health or epidemiological purposes, health care treatment, insurance, payment or operations under the federal Health Insurance Portability and Accountability Act of 1996, or to X-ray, roentgen process, computed tomography, MRI, PET scan, mammography or other image or film of the human anatomy used exclusively to diagnose, prognose or treat an illness or other medical condition or to further validate scientific testing or screening;

(2) Individuals sharing their personal contact information such as electronic mail addresses with other individuals in the workplace, or other social, political or similar settings where the purpose of the information is to facilitate communication among such individuals, provided sections 1 to 18, inclusive, of this act shall cover any processing of such contact information beyond interpersonal communication; and

(3) Covered entities' publication of entity-based member or employee contact information where such publication is intended to allow members of the public to contact such member or employee in the ordinary course of the entity's operations.

Sec. 18. (NEW) (Effective July 1, 2022) (a) The provisions of sections 1
to 18, inclusive, of this act shall supersede local or state laws, regulations and ordinances, except when such local or state laws, regulations or ordinances provide stronger privacy protections for individuals.

(b) Sections 1 to 18, inclusive, of this act cover businesses that are subject to federal laws concerning the processing of individuals’ personal information to the extent that (1) sections 1 to 18, inclusive, of this act provide stronger privacy protections for individuals than those federal laws; and (2) those federal laws do not explicitly preempt state laws.

Sec. 19. (Effective from passage) (a) The commission shall conduct a study to determine the most effective way for covered entities to obtain individuals’ consent in accordance with section 5 of this act for each type of personal information processing. The commission may request data and information from covered entities conducting business in the state, governmental entities, consumer protection experts, privacy advocates, researchers and other relevant sources for purposes of the study.

(b) Not later than February 1, 2022, the commission shall submit a report, in accordance with the provisions of section 11-4a of the general statutes, to the joint standing committee of the General Assembly having cognizance of matters relating to general law concerning the findings of such study."

This act shall take effect as follows and shall amend the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Effective Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sec. 1</td>
<td>from passage</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 2</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 3</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 4</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 5</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 6</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 7</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 8</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 9</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 10</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 11</td>
<td>January 1, 2023</td>
<td>New section</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Sec. 12</td>
<td>from passage</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 13</td>
<td>January 1, 2023</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 14</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 15</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 16</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 17</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 18</td>
<td>July 1, 2022</td>
<td>New section</td>
</tr>
<tr>
<td>Sec. 19</td>
<td>from passage</td>
<td>New section</td>
</tr>
</tbody>
</table>