OLR Bill Analysis

sSB 1356

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

SUMMARY

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

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

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

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

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

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

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

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

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

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

§§ 1-9 — CTDPA

Expansion of Applicability

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

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

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

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

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

The bill also extends the CTDPA to cover those that (1) control or

process a consumer's sensitive data (see below) or (2) offer a consumer's personal data for sale in trade or commerce.

Sensitive Data

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

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

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

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

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

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

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

The bill also includes the following as sensitive data:

1. neural data (any information generated by measuring the activity

of an individual's central or peripheral nervous system);

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

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

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

Publicly Available Information

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

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

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

1. information compiled and combined to create a consumer profile made available to a user of a publicly available Internet website either for payment or free of charge,

2. information that is made available for sale, or

3. any inference generated from the information described above.

Consumer Health Data

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

Exemption Removal

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

1. nonprofit organizations;

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

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

Consumer Rights

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

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

The bill also gives a consumer the right to obtain from the controller (1) a list of the third parties to whom the controller has sold the

consumer's personal data or (2) if the controller does not maintain such a list, a list of all third parties to whom the controller has sold personal data.

Controller Requirement

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

§§ 1 & 4-9 — KNOWLEDGE FAIRLY IMPLIED

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

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

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

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

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

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

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

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

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

§§ 6 & 10 — INTERNAL OPERATIONS

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

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

Social Media Platform

Under current law, a "social media platform" is a public or semi-public Internet-based service or application that:

1. is used by a Connecticut consumer;

2. is primarily intended to connect and allow users to socially

interact within the service or application; and

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

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

Prohibition on Requiring Social Media Account for Request

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

Rebuttable Presumption

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

Consent Provision Eliminated

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

The following actions are prohibited under current law unless the

requisite consent is received, but under the bill no one can consent to them:

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

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

Automated Decisions

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

Precise Geolocation

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

§ 11 — BROKERED PERSONAL DATA

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

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

A "business" is (1) a person (i.e. individual or entity) that regularly engages in commercial activities to generate income; (2) a bank, Connecticut credit union, federal credit union, out-of-state bank, out-of-state trust company, or out-of-state credit union; and (3) any other person that controls, is controlled by or is under common control with

a person described above. A business does not include any state body, authority, board, bureau, commission, district, or agency of the state or its political subdivisions.

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

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

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

Application

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

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

1. the applicant's name, mailing address, email address, telephone

number, and primary Internet website address and

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

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

Data Sale Prohibition

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

Exemptions

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

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

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

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

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

Unregistered Data Broker's Permitted Actions

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

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

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

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

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

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

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

Regulations

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

Penalties

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

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

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

sending commands to, a vehicle.

Definitions

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

A "covered act" is an action that constitutes:

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

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

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

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

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

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

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

Survivor's Connected Vehicle Service Request

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

include at least the following, as applicable:

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

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

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

Covered Provider Required Actions

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

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

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

3. if the motor vehicle has an in-vehicle interface, informing the survivor about the interface's availability, and providing information on how to use it to terminate or disable the connected vehicle services.

Denial of Abuser Request

After the covered provider has acted, the provider must deny any request the abuser makes to obtain data (1) generated by the connected vehicle service after the abuser's access to the service was terminated or

disabled due to the survivor's request and (2) that the covered provider maintains.

Covered Provider's Requirement to Act

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

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

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

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

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

Notice to Survivor Required Before Notifying Abuser

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

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

When Action is Not Operationally or Technically Feasible

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

Confidentially of Request-Related Information

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

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

Material Change Notifications

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

Emergency Situations

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

Website Instructions

The bill requires each covered provider to publicly post on its website a statement describing how a survivor may submit a connected vehicle service request to the provider.

BACKGROUND

Related Bills

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

certain actions, thus prohibiting the controllers from taking such actions.

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

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

COMMITTEE ACTION

General Law Committee

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