OLR Bill Analysis

sSB 1356 (File 609, as amended by Senate "A")*

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. requires an impact assessment for controllers or processors that do certain profiling (i.e. automated processing of personal data to evaluate or predict an individual's personal characteristics, such as economic situation, health, personal preferences or location);

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

4. 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;

5. changes the standard for establishing knowledge of a consumer's minor-status (i.e. under age 18) as it pertains to certain requirements and restrictions by creating a new "fairly implied knowledge" standard (see below);

6. 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; and

7. prohibits direct messaging unless there is a safeguard that prevents unconnected adults from sending unsolicited communications to a minor and requires this to be the social media platform's default setting.

Additionally, the bill (1) requires social media platform owners, by January 1, 2026, to incorporate an online safety center and create a policy for handling reports of cyberbullying on the platform and (2) generally requires a data broker to be actively registered with the Department of Consumer Protection 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 legally under the survivor's exclusive possession or control.

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

*Senate Amendment "A" (1) eliminates the minimum amount of personal data a person or group of persons was required to control or process, based on gross revenue, that was required to qualify as a controller; (2) modifies certain definitions and exemptions; (3) adds provisions on profiling and impact assessments; (4) modifies certain consumer and controller rights under the CTDPA; (5) modifies what is considered a heightened risk to minors; (6) adds provisions on social media platform online safety centers and cyberbullying policies; (7) increases the data broker registration fee from $600 to $1,200, and (8) makes numerous minor, technical, and conforming changes.

EFFECTIVE DATE: February 1, 2026, except (1) October 1, 2025, for the online safety center, cyberbullying policy, and brokered personal data provisions; and (2) January 1, 2026, for the motor vehicle data privacy provision.

§§ 2-9 & 15 — CTDPA

Expansion of Applicability (§ 3)

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 the first threshold to 35,000 consumers and eliminates the second. It also extends the CTDPA to apply to persons that (1) control or process consumers' sensitive data (see below) or (2) offer consumers' personal data for sale in trade or commerce.

Profiling (§§ 2, 5, 8, 9 & 15)

Under existing law, unchanged by the bill, "profiling" is any form of automated processing done on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Decision That Produces Any Legal or Similarly Significant Effect. Under current law, "decisions that produce legal or similarly significant effects concerning a consumer" are controllers' decisions that result in providing or denying financial or lending services, housing,

insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services. The bill expands this to also include any decision made on the controller's behalf that has this effect.

Opt-out. The bill 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. If the consumer's personal data were processed for profiling purposes to further any such automated decision concerning the consumer and, if feasible, the consumer has the right to:

1. question the result of the profiling;

2. be informed of the reason that the profiling resulted in the decision;

3. review his or her personal data that were processed for the profiling; and

4. correct any incorrect personal data that were processed for profiling purposes and have the profiling decision reevaluated based on the corrected personal data, if the profiling decision concerns housing, taking into account the nature of the personal data and why the personal data were processed.

Impact Assessments. Under the bill, each controller that engages in any profiling for the purposes of making a decision that produces any legal or similarly significant effect related to a consumer must conduct an impact assessment for the profiling. The impact assessment must include the following, to the extent reasonably known by or available to the controller, as applicable:

1. a statement by the controller disclosing the profiling's purpose, intended use cases and deployment context, and benefits;

2. an analysis of whether the profiling poses any known or reasonably foreseeable heightened risk of harm to a consumer

(see below), and, if so, the (a) nature of the risk and (b) necessary mitigation steps;

3. a description of the (a) main categories of personal data processed as inputs for the profiling and (b) outputs the profiling produces;

4. an overview of the main categories of personal data the controller used to customize the profiling, if applicable;

5. any metrics used to evaluate the performance and known profiling limitations;

6. a description of any transparency measures taken concerning the profiling, including any taken to disclose to consumers that the controller is engaged in the profiling while so engaged; and

7. a description of the post-deployment monitoring and user safeguards provided concerning the profiling, including the oversight, use, and learning processes the controller established to address issues arising from the profiling.

The bill applies to these impact assessments provisions that apply to data protection assessments under existing law, such as allowing (1) the attorney general to require certain disclosures, (2) a single assessment to address comparable operations with similar activities, and (3) compliance with another applicable law or regulation to satisfy CTDPA requirements.

Under the bill, these impact assessment requirements apply to processing activities created or generated on or after March 1, 2026, and are not retroactive.

Under existing law, "heightened risk of harm to a consumer" generally includes the (1) processing of personal data for the purpose of targeted advertising; (2) sale of personal data; (3) processing of personal data for the purpose of profiling, where the profiling presents a reasonably foreseeable risk; or (4) processing of sensitive data.

Ability to Collect, Use, or Retain Data. The bill specifies that the obligations it imposes on controllers, processors, or consumer health data controllers do not restrict their ability to collect, use, or retain data for internal use to process personal data for profiling purposes to further any automated decision that may produce any legal or similarly significant effect concerning a consumer, if the personal data are:

1. processed only to the extent necessary to detect or correct any bias that may result from processing the data for profiling purposes, the bias cannot effectively be detected or corrected without processing the data, and the data are deleted once the processing has been completed;

2. processed subject to appropriate safeguards to protect the consumers' rights under the U.S. or state constitutions or laws;

3. subject to technical restrictions concerning the reuse of the data and industry-standard security and privacy measures, including pseudonymization;

4. subject to measures to ensure that the data are secure, protected, and subject to suitable safeguards, including strict data access controls and related documentation, to avoid misuse and limit data access to authorized individuals only while preserving the data's confidentiality; and

5. not transmitted or transferred to, or otherwise accessed by, any third party.

The bill also allows the controllers, processors, or consumer health data controllers to collect, use, or retain data for internal operations, consistent with COPPA's internal operations exception, when processing data under that exception.

Sensitive Data (§§ 2 & 6)

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.

Under existing 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 also 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 processed data used to uniquely identify an individual; and

3. including personal data collected from an individual who is a child and the controller's knowledge of such is fairly implied on the basis of objective circumstances, rather than based only on the controller's actual knowledge as under current law.

Under the bill, the following are also considered sensitive data:

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

2. a consumer's financial account number or 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 the consumer's financial account; or

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

Publicly Available Information (§ 2)

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, information is considered publicly available if either one of these requirements is satisfied, rather than both. Simultaneously, for widely distributed media information, the bill only requires that the controller has a reasonable basis to believe that the information has been lawfully made available to the general public. Under existing law, publicly available information is not "personal data" and is, therefore, not subject to the CTDPA.

The bill specifies that any biometric data that can be associated with a specific consumer and were collected without the consumer's consent is not considered publicly available information.

Consumer Health Data (§ 2)

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.

Exemptions (§ 4)

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).

The bill also exempts the following from CTDPA:

1. candidate committees, national committees, party committees, or political committees;

2. insurers or their affiliates, fraternal benefit societies, insurance-support organizations, insurance agents, or insurance producers;

3. various banks, financial institutions (e.g., credit unions) or their affiliates or subsidiaries that (a) are only and directly engaged in financial activities as described in federal banking law, (b) are regulated and examined by the Banking Department or an applicable federal banking regulatory agency, and (c) have established a program to comply with applicable federal or state personal data-related requirements; or

4. agents, broker-dealers, investment advisers, or investment adviser agents who are regulated by the banking department or the federal Securities and Exchange Commission.

Current law exempts certain information and data from CTDPA, including those related to protecting human subjects under certain federal Food and Drug Administration-related regulations. The bill specifies that this exemption only applies to personal data for these protection purposes.

The bill also exempts (1) financial institutions' customers' protected nonpublic personal information subject to the Gramm-Leach Bliley Act and (2) a covered entity's (see above) limited data set (i.e. protected health information that excludes specific identifiers) that are used,

disclosed, and maintained for purposes such as research, public health, or health care operations (45 C.F.R. § 164.514(e)).

Consumer Rights (§ 5)

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 are derived from the personal data and whether a controller or processor is processing the consumer's personal data for profiling purposes to make a decision that produces any legal or similarly significant effect on a consumer (as defined above). 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 the exception to include when a controller is prohibited from disclosing certain personal information under the bill.

As under existing law for other requests, if a controller, using commercially reasonable efforts, cannot authenticate a consumer's request, the controller is not required to comply with the request to initiate an action under this provision. The controller must notify the consumer that it is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the consumer and his or her request.

Under the bill, a controller is prohibited from disclosing certain personal data in response to a consumer's request to confirm whether data is being processed and to access the data. The controller must instead inform the consumer or person acting on his or her behalf, with sufficient particularity, that the controller has collected the personal data on the consumer's (1) Social Security number; (2) driver's license, state identification card, or other government-issued identification numbers; (3) financial account number; (4) health insurance or medical identification numbers; (5) account password; (6) security question or its answer; or (7) biometric data.

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, however, the controller is not required to reveal any trade secret.

Controller Requirements (§ 6)

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 limits the data collection to what is reasonably necessary and proportionate to the disclosed purpose for processing the data.

Current law prohibits controllers from processing personal data for purposes that are neither reasonably necessary to, nor compatible with, the purposes disclosed to the consumer, except with the consumer's consent. Under the bill, before processing a consumer's personal data for a material new purpose the controller must consider the consumer's reasonable expectation regarding the personal data at the time they were collected based on the disclosed purposes. The controller must also consider the following:

1. the relationship between the new purpose and the purposes that were disclosed to the consumer;

2. the impact that processing the personal data for the new purpose might have on the consumer;

3. the relationship between the consumer and the controller and the context in which the personal data were collected; and

4. whether there are any additional safeguards, including encryption or pseudonymization, in processing the personal data for the new purpose.

Under current law, controllers are prohibited from processing sensitive data (see above) without consumer consent or, in the case of children, in accordance with COPPA. The bill further limits controllers from doing so unless it is reasonably necessary in relation to the purposes for which the sensitive data are processed.

Current law prohibits controllers from processing personal data in violation of state laws that prohibit unlawful discrimination against consumers. The bill specifies that the prohibition against processing personal data in violation of any such state law also applies to any evidence, or lack of evidence, on proactive anti-bias testing or similar efforts to avoid processing the data in violation of the law. The quality, efficacy, recency, and scope of the test or effort; the results of the test or effort; and the response to these results, are relevant to any claim available for a violation and any defense.

Privacy Notice and Disclosure (§ 6)

Existing law requires controllers to provide consumers with a reasonably accessible, clear, and meaningful privacy notice. The bill modifies the required notice in various ways as described below.

Notice on Third Parties and Targeted Advertising. Current law requires the notice to include the categories of personal data the controller shares with third parties and the categories of third parties with whom the controller shares personal data. Under the bill, this pertains to data the controller sells instead of what is shared as under current law.

Under current law, if a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose the processing. The bill requires this disclosure to be included in the privacy notice.

Additional Privacy Notice Content. The bill also requires the controller to include the following information in the notice:

1. disclosure of whether the controller collects, uses, or sells personal data to train large language models; and

2. the most recent month and year during which the controller updated the privacy notice.

Under the bill, a controller must make the required privacy notice publicly available:

1. through a conspicuous hyperlink that includes the word "privacy" (a) on the homepage of the controller's website, if the controller maintains one; (b) on a mobile device's application store page or download page, if maintained by the controller; and (c) on the application's settings menu or in a similarly conspicuous and accessible location, if the controller maintains an application for use on a mobile device or other device used to connect to the Internet;

2. through a medium where the controller regularly interacts with consumers, including mail, if the controller does not maintain a website;

3. in each language in which the controller (a) provides any product or service that is subject to the privacy notice, or (b) carries out any activity related to any such product or service; and

4. in a way that is reasonably accessible to, and usable by, individuals with disabilities.

Notice of Retroactive Material Change. Whenever a controller makes any retroactive material change to the privacy notice or practices, the bill requires the controller to:

1. notify affected consumers regarding any personal data to be collected after the change's effective date; and

2. provide a reasonable opportunity for these consumers to withdraw consent to any further and materially different collection, processing, or transfer of previously collected personal data following the material change.

The controller must also take all reasonable electronic measures to provide the notice to affected consumers, considering the available technology and the nature of the controller's relationship with the affected consumers.

Connecticut-Specific Notice Not Required. The bill specifies that it should not be construed to require a controller to provide a privacy

notice that is specific to Connecticut if the controller provides a generally applicable privacy notice that satisfies the established requirements.

Opt-Outs (§ 6)

Under current law, the secure and reliable means required for a consumer to exercise their rights described above must include a clear and conspicuous link on the controller's website to a website that enables a consumer or the consumer's agent to opt out of the targeted advertising or sale of the consumer's personal data.

The bill specifically allows consumers to opt-out of the processing of the consumer's personal data for targeted advertising and personal data sale purposes.

Processors Assistance to Controllers (§ 7)

Under current law, a processor must assist the controller in meeting the controller's obligations under CTDPA, while considering the nature of processing and the information available to the processor by appropriate technical and organizational measures, as reasonably practicable, to fulfill the controller's obligation to respond to a request from a consumer exercising his or her rights under CTDPA.

The bill eliminates the requirement that processors take into account the appropriate technical and organizational measures and only requires them to assist if possible, rather than when it is reasonably practicable.

Existing law requires processors to also assist by providing necessary information to enable controllers to conduct and document data protection assessments. The bill also requires this assistance regarding impact assessments.

§§ 10-15 — MINORS AND SOCIAL MEDIA PLATFORMS, ONLINE SERVICES, PRODUCTS, AND FEATURES

Heightened Risk of Harm to Minors (§ 11)

Existing law requires a controller with consumers who are minors to use reasonable care to avoid causing any heightened risk of harm to

minors in processing personal data. The bill broadens what constitutes "heightened risk of harm to minors" by also including the foreseeable risk of the following:

1. any physical violence against minors;

2. any material harassment of minors on any online service, product, or feature, where it is severe, pervasive, or objectively offensive to a reasonable person; or

3. any sexual abuse or sexual exploitation of minors.

Under current law, heightened risk of harm to minors includes the foreseeable risk of any (1) unfair or deceptive treatment of, or any unlawful disparate impact on, minors; (2) financial, physical, or reputational injury to minors; or (3) physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of minors if the intrusion would be offensive to a reasonable person. Under the bill, the injury or intrusion must be material.

In doing so, the bill requires controllers to do additional data protection assessments for these new risk factors and make and implement plans to mitigate or eliminate the risk. By law, each controller with consumers who are minors must (1) do a data protection assessment of its online service, product, or feature to address any heightened risk of harm to minors that is a reasonably foreseeable result of offering the online service, product, or feature to minors and (2) make and implement a plan to mitigate or eliminate the risk.

By law, an "online service, product, or feature" is any service, product, or feature provided online, but not telecommunications or broadband Internet access service, or delivery or use of a physical product.

Prohibition on Requiring Social Media Account for Request (§ 10)

Existing law requires social media platforms to unpublish a minor's social media account within 15 business days, and generally delete the account within 45 business days, after receiving an authenticated

request. The bill prohibits social media platforms from requiring a minor's parent or legal guardian to create a social media account to submit such a request. 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.

Knowledge Fairly Implied (§§ 5, 6, 12 & 13)

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 on the basis of 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. 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;

2. 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;

3. 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; and

4. prohibiting controllers from processing a consumer's personal data for targeted advertising, or selling the data without the consumer's consent, for certain minor consumers.

The bill also includes 16- and 17-year-olds in the last prohibition, which only applies to 13- to 16-year-olds under current law.

Consent Provision Eliminated (§ 12)

Currently, controllers that offer an online service, product, or feature to minors may take certain actions if they receive the minor's consent or, if the minor is younger than age 13, the minor's parent or legal guardian's consent. The bill eliminates the ability for someone to consent for these provisions, thus generally prohibiting them.

Specifically, under the bill, these controllers are now generally prohibited from:

1. processing any minor's personal data for targeted advertising and personal data sales 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.

Precise Geolocation (§ 12)

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, necessary for the controller to provide the online service, product, or feature.

Automated Decisions (§ 12)

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.

Unsolicited Communications to Minors (§ 12)

The bill prohibits a controller from offering direct messaging unless it provides readily accessible and easy-to-use safeguards to allow a minor or a minor's parent or legal guardian to prevent adults that the minor is not connected with from sending unsolicited communications to the minor. It also requires this safeguard to be the default setting. Under current law, controllers only need to offer readily accessible and easy-to-use safeguards to limit an adult's ability to send these unsolicited communications.

Features Designed to Increase Use (§ 12)

Current law prohibits a controller from using any system design feature to significantly increase, sustain, or extend the use of an online service, product, or feature, without first getting the minor's consent or, if the minor is younger than age 13, the minor's parent or legal guardian's consent. The bill prohibits this type of feature by removing the ability for someone to consent to it.

Educational Exception. The bill allows an educational entity, including a learning management system or a student engagement program, to use a service or application designed to significantly increase, sustain, or extend the use of the online service, product, or feature.

Impact Assessment (§§ 13 & 14)

The bill requires an impact assessment for any controller that offers any online service, product, or feature to a minor if it does any profiling based on the consumer's personal data. The controller must do these assessments if it has actual knowledge, or has knowledge fairly implied based on objective circumstances, that the consumer is a minor. It requires a processor to provide any information that is needed for a controller to conduct and document an impact assessment. As under existing law, processors must adhere to a controller's instructions and assist the controller in meeting its obligations under CTDPA.

Requirements. The impact assessment must include, to the extent reasonably known by or available to the controller or processor, as applicable:

1. a statement disclosing the purpose, intended use cases and deployment context of, and benefits afforded by, the online service, product, or feature, if it engages in any profiling to make decisions that produce legal or similarly significant effects about consumers;

2. an analysis of whether the profiling poses any known or reasonably foreseeable heightened risk of harm to minors and, if so, the nature of the risk and the steps taken to mitigate it;

3. a description of the (a) personal data categories the online service, product, or feature processes as inputs for the profiling, and (b) resulting outputs the service, product, or feature produces;

4. an overview of the personal data categories used to customize the online service, product, or feature for the profiling, if any were used;

5. a description of any transparency measures taken on the online service, product, or feature about the profiling, including those to inform consumers that the service, product, or feature is being used for the profiling while it is occurring; and

6. a description of the post-deployment monitoring and user safeguards provided about the online service, product, or feature for the profiling, including the oversight, use, and learning processes established to address issues from deploying the service, product, or feature for the profiling.

The bill imposes the same requirements to these impact assessments as existing law imposes on a controller for a data protection assessment.

Review and Retention. The controller must (1) review the assessment as needed to account for any material change to the profiling operations of the online service, product, or feature that is the subject of

the assessment and (2) keep documentation on the assessment for the longer of (a) three years, beginning when the profiling operation ends or (b) as long as the service, product, or feature is offered.

Single Assessment. The bill allows a single impact assessment to address a comparable set of profiling operations that include similar activities. And if a controller does an assessment to comply with another law or regulation, that assessment satisfies the bill's assessment requirement if it is reasonably similar in scope and effect.

Plan to Mitigate or Eliminate Risk. Additionally, for controllers with assessments that show their online service, product, or feature poses a heightened risk to minors, the bill requires them to make and implement a plan to mitigate or eliminate the risk.

The bill also allows the attorney general to require a controller to disclose to him a plan to mitigate or eliminate the risk, for both data protection assessments and impact assessments, if the plan is relevant to an attorney general investigation. The controller must disclose the plan within 90 days of the attorney general notifying the controller of the required disclosure.

Exempt From Disclosure. As is the case under existing law for data protection assessments, under the bill, impact assessments and harm mitigation or elimination plans are confidential and exempt from disclosure under the Freedom of Information Act. If any information in an assessment or plan is disclosed to the attorney general and subject to the attorney-client privilege or work product protection, the disclosure does not waive the privilege or protection.

Internal Operations (§ 15)

The CTDPA specifies that the obligations it imposes on controllers or processors who offer online services, products, or features to minors, 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.

§ 1 — SOCIAL MEDIA PLATFORM OWNER REQUIREMENTS

Online Safety Center

The bill requires each social media platform owner, by January 1, 2026, to incorporate an online safety center into the platform. An online safety center must at least give consumers who live in Connecticut and use the platform the following:

1. resources to (a) prevent cyberbullying on the platform and (b) enable them to identify ways to get mental health services, including a website address or telephone number to get services to treat an anxiety disorder or suicide prevention;

2. access to online behavioral health educational resources;

3. an explanation of the platform's mechanism for reporting harmful or unwanted behavior, including cyberbullying on the platform; and

4. educational information about social media platforms' impact on users' mental health.

Under law and the bill, a "social media platform" is a public or semi-public Internet service or application used by a Connecticut consumer that:

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

2. enables a user to (a) construct a public or semi-public profile to sign into and use 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 seen by other users, including on message boards, in chat rooms, or through a landing page or main feed that also presents content from other users.

It is not a public or semi-public Internet service or application that:

1. only provides e-mail or direct messaging;

2. primarily has news, sports, entertainment, interactive video games, electronic commerce, or content the provider preselects or for which any chat, comments, or interactive functionality is incidental or directly related to, or dependent on, providing the content; or

3. is used by and under an educational entity's direction, including a learning management system or student engagement program.

Cyberbullying Policy

The bill similarly requires each social media platform owner, by January 1, 2026, to establish a cyberbullying policy with a process for the owner to handle reports of cyberbullying on the platform. Cyberbullying is any act that (1) is reasonably likely to cause physical or emotional harm to a consumer or place him or her in fear of physical or emotional harm, or (2) infringes on a consumer's rights under state or federal law.

§ 16 — BROKERED PERSONAL DATA

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.

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 $1,200 registration fee. A registration expires on December 31 of the year in which it was issued and may be annually renewed for a $1,200 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 state Uniform Administrative Procedure Act, may impose maximum civil penalties of $500 per day for each data broker violation, up to $10,000 per calendar year.

§ 17 — 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 of 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.

Immunity

The bill provides immunity from civil liability to each covered provider and its officers, directors, employees, vendors, or agents for any act or omission they commit under this provision if the act or omission was committed to comply with the provision.

BACKGROUND

Related Bills

sSB 2 (File 603), as amended by Senate "A" and "B," and passed by

the Senate, has substantially similar CTDPA exemptions.

sSB 1295 (File 576), favorably reported by the General Law Committee, among other things, has similar provisions to this bill, including requiring social media platforms to have an online safety center and a cyberbullying policy, changing the knowledge standard for determining a consumer's status as a minor, prohibiting controllers from taking certain actions, prohibiting certain direct messages, and requiring impact assessments for profiling based on a minor's personal data.

HB 5474 (File 184), favorably reported by the Committee on Children, among other things, adds additional protections 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 (File 677), favorably reported by the Government Administration and Elections Committee, removes existing law's provisions that exempt the state from the CTDPA.

COMMITTEE ACTION

General Law Committee

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

Judiciary Committee

Joint Favorable
Yea 28 Nay 9 (04/25/2025)

Appropriations Committee

Joint Favorable
Yea 38 Nay 12 (05/05/2025)