OLR Bill Analysis

sSB 4 (File 285, as amended by Senate "A")*

AN ACT CONCERNING CONSUMER PRIVACY AND PROTECTION.

TABLE OF CONTENTS:

SUMMARY

This bill makes various unrelated changes related to consumer privacy and protection, as described in the section-by-section analysis below.

*Senate Amendment "A" (1) removes the provisions on tariffs, automatic license plate readers, and denied employment based on automated profiling; (2) modifies the provisions on data brokers, algorithmic pricing, and the Connecticut Data Privacy Act (CTDPA); (3) adds the provisions on genetic testing and advertisement volume; and (4) makes various minor, technical, and conforming changes.

EFFECTIVE DATE: October 1, 2026

§§ 1-10 — DATA BROKERS

Requires data brokers to register with DCP; establishes a deletion mechanism program for consumers to request that data brokers delete their personal data; requires data brokers to check the program once every 45 days; creates a civil penalty of up to $200 per day per violation

Licensing (§§ 1 & 2)

The bill generally requires data brokers who sell or license brokered data in the state on or after January 1, 2027, to be actively registered with the Department of Consumer Protection (DCP).

Under the bill, "brokered personal data" is one or more of the following personal data elements concerning a consumer, if categorized or organized for sale or license to a third party:

1. name;
2. address;
3. birthday;
4. birthplace;
5. mother's maiden name;
6. unique biometric data (a) generated from measurement or technical analysis of a human body characteristic, including a fingerprint, retina, iris image, or other unique physical or digital representation of biometric data, and (b) used by the owner or licensee to identify or authenticate the consumer;
7. name or address of a consumer's immediate family or household

member;

8. Social Security number or other government-issued identification number; or

9. other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

These data brokers must submit to DCP, as the commissioner requires, an application for an initial registration with a $2,500 initial registration fee. The initial registration expires on December 31 of the year it is issued and may be renewed for successive one-year terms. The renewal application must be made in the same way as an initial application and with a $2,500 renewal fee. All these fees are deposited in the data broker registration account the bill establishes (see below).

All applications must disclose:

1. the applicant's name, mailing address, and an actively monitored email address and telephone number;

2. the applicant's primary website address;

3. a publicly accessible webpage address on the applicant's primary website that (a) does not make use of any dark pattern (a user interface designed with the substantial effect of subverting or impairing user autonomy, decision-making, or choice) and (b) details how a consumer may exercise each of their rights under the CTDPA (see BACKGROUND);

4. whether the applicant collects (a) minors' personal data or (b) consumers' precise geolocation data or reproductive or sexual health data;

5. the measures the applicant must take to ensure that no personal data is sold or licensed in violation the bill's data broker provisions and the CTDPA;

6. if, and to what extent, the applicant or any of its subsidiaries is regulated under the (a) Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.); (b) Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and its regulations; (c) Insurance Data Security Law (CGS § 38a-38); or (d) privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services (45 C.F.R. Parts 160 and 164);

7. for renewals submitted on or after July 1, 2029, the statement the applicant most recently posted on a publicly accessible webpage on their primary website as required by the bill (see § 6 below);

8. for renewals submitted on or after July 1, 2031, (a) whether the applicant has undergone an audit as required by the bill (see § 5 below) and (b) if so, the most recent audit report and related materials; and

9. any other information the DCP commissioner requires.

The bill also allows DCP to approve and renew a data broker registration under the terms of an agreement between the department and the Nationwide Multistate Licensing System.

Prohibition on Selling Personal Data (§ 3)

The bill prohibits data brokers from selling or licensing any personal data in violation of the bill's data broker provisions and the CTDPA. Each registered data broker must have a privacy policy that at least includes measures to ensure compliance with this prohibition.

Deletion Mechanism (§ 5)

The bill requires the DCP commissioner, by July 1, 2028, to establish an accessible deletion mechanism program. The program must have an accessible deletion mechanism that:

1. allows a consumer for whom a registered data broker has collected personal data to (a) submit a free deletion request, in a commissioner-prescribed verifiable way and in any language a consumer speaks, to have all registered data brokers and data

service providers delete their personal data and (b) specifically exclude one or more registered data brokers, and all applicable data service providers, from the deletion request;

2. allows a consumer to (a) securely submit additional personal data (including a driver's license) to help process the deletion request, (b) check the deletion request status, and (c) submit updates to the verified deletion request no more than once in any 45-day period;

3. allows a registered data broker to determine whether a consumer has specifically excluded the broker and the broker's data service providers from the deletion request or any update;

4. prohibits a registered data broker that accesses the deletion mechanism for determining whether it has been excluded to access any additional personal data through the deletion mechanism;

5. is readily accessible and usable by consumers with disabilities;

6. incorporates reasonable security safeguards, including administrative, physical, and technical safeguards, to protect consumers' personal data from any unauthorized use, disclosure, access, destruction, or modification through the deletion mechanism; and

7. gives consumers, in a readily understandable way, (a) a description of what is considered personal data and may be deleted if requested, (b) an explanation of the deletion request process, and (c) a description of the actions the bill requires for brokers to delete personal data.

If a consumer submits his or her driver's license number to the commissioner to verify the deletion request or update it, the commissioner must only use the number for that purpose. He must not share, store, or retain the number.

Each deletion or update request is confidential and is not deemed a

public request under the Freedom of Information Act.

Verification

Beginning on August 15, 2028, the DCP commissioner or his authorized agent must verify that the consumer actually submitted the deletion request or update by using the consumer's driver's license number and then update the deletion mechanism and inform each registered broker that accesses the mechanism that the request or update has been verified.

If the commissioner or his authorized agent cannot verify the request or update, then they must specify that all registered data brokers and their data service providers that are not specifically excluded from the unverified deletion request or update (1) may retain any personal data on the consumer and (2) must process the unverified deletion request or update as an exercise of the consumer's rights under the CTDPA to opt-out of personal data processes for certain purposes, such as targeted advertisement.

Broker Deletion Requirements

Beginning October 1, 2028, each registered data broker must access the accessible deletion mechanism at least once every 45 days to examine each deletion request or update to determine whether the broker and its data service providers are specifically excluded from that request or update.

For each verified deletion request or update that does not specifically exclude the broker and its data service providers, the broker must generally delete any personal data it maintains on the consumer and direct all data service providers with any of the consumer's personal data held on the broker's behalf to also do so.

For each unverified deletion request or update that does not specifically exclude the broker and its data service providers, the broker must (1) retain any personal data the broker has about the consumer and (2) process the unverified deletion request or update, and direct all of its data service providers to process the unverified request or update, as an

exercise of the consumer's rights under the CTDPA to opt-out of personal data processes for certain purposes.

The bill also generally requires brokers, at least once every 45 days after it first deletes a participating consumer's personal data, to repeat the bill's required actions for a verified request or update. Brokers do not have to do this if the:

1. broker verifies that the participating consumer submitted a verified update to a verified deletion request and

2. verified update specifically excludes the broker and all its data service providers from the updated deletion request.

Allowable DCP Fee

The bill allows the DCP commissioner to impose a fee on each registered data broker that accesses the accessible deletion mechanism to perform its duties after a deletion request or update. The commissioner determines the fee amount, but it must not exceed the cost of providing the service. Collected fees must be deposited in the data broker registration account the bill establishes (see below).

Subsequently Acquired Data Prohibition

The bill generally prohibits, beginning October 1, 2028, registered data brokers and their data service providers that delete a participating consumer's personal data from maintaining, using, or disclosing any personal data they subsequently acquire about the participating consumer.

Excepted Circumstances

1. Under the bill, a registered data broker who maintains a participating consumer's personal data and its data service providers do not have to delete a consumer's personal data, and may maintain, use, or disclose it, when it is reasonably necessary to:

2. comply with any federal, state, or municipal law, ordinance, or regulation;

3. comply with any civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by any federal, state, municipal, or other governmental authority;

4. cooperate with any law enforcement agency about any conduct or activity that the registered data broker or data service provider reasonably and in good faith believes may violate any federal, state, or municipal law, ordinance, or regulation;

5. investigate, establish, exercise, prepare for, or defend any legal claim;

6. provide any product or service the participating consumer specifically requests;

7. perform any contract where the participating consumer is a party, including fulfilling written warranty terms;

8. take any step at the participating consumer's request to enter a contract;

9. take any immediate step to protect any interest that is essential for the life or physical safety of the participating consumer or another person;

10. prevent, detect, protect against, or respond to any security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity; preserve the integrity or security of any system; or investigate, report, or prosecute those responsible for these actions;

11. engage in any public or peer-reviewed scientific or statistical research in the public interest that follows all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines, or has a similar independent oversight entity that determines, that (a) maintaining the participating consumer's personal data is likely to provide substantial benefits that do not exclusively benefit the registered data broker or data service provider, (b) the expected

benefits of the research outweigh the privacy risks, and (c) the broker or data service provider has implemented reasonable safeguards to mitigate privacy risks associated with the research;

12. help any other person in performing any obligation imposed by the bill's data broker provisions;

13. do internal research to develop, improve, or repair any product, service, or technology;

14. carry out a product recall;

15. identify and repair any technical error that impairs existing or intended functionality; or

16. perform internal operations that are reasonably aligned with the expectations the participating consumer had, or reasonably anticipated, based on the consumer's existing relationship with the broker.

The bill generally prohibits registered data brokers or their data service providers from maintaining, using, or disclosing the participating consumer's personal data for any other purpose.

Audit

The bill generally requires, beginning July 1, 2031, and every three years after, registered data brokers to:

1. have an independent auditor audit their books to determine their compliance with the bill's deletion mechanism requirements, prepare an audit report disclosing the results, and submit the report and any associated materials to the broker; and

2. maintain each audit report and associated materials for at least six years from when they are submitted to the broker.

The bill generally requires a registered data broker to submit the audit report and the materials to DCP within five business days after the department sends notice to the broker it must do so.

DCP Contract for Implementation

The bill allows the DCP commissioner to contract with one or more public or private entities (1) for any services needed to implement these provisions or (2) to run the accessible deletion mechanism program or a multistate accessible deletion mechanism.

DCP Website (§ 4)

The bill requires the DCP commissioner to make, and periodically update, a webpage on the department's website that (1) discloses for each registered data broker, the information in the broker's most recent approved application and (2) provides access to the accessible deletion mechanism established by the commissioner.

Data Broker Website Disclosures (§ 6)

The bill generally requires, by July 1, 2029, each business that was a registered data broker during the prior calendar year to annually post, in a commissioner-prescribed way and on a publicly accessible webpage on the business's primary website, a statement disclosing the following information:

1. the total number of deletion requests, including any updates, that the business accessed during the prior year and that did not specifically exclude the business and its data service providers;

2. the total number of deletion requests to which the business responded by (a) deleting personal data, (b) retaining personal data, or (c) deleting some and retaining other personal data; and

3. if the business responded to one or more deletion requests by retaining personal data, the total number of the deletion requests for which it kept personal data based on the (a) excepted circumstances listed above or (b) exemptions listed below.

Exemptions (§ 7)

The bill's data broker provisions do not apply to:

1. a consumer reporting agency, a person who furnishes information to a consumer reporting agency, or a user of a

consumer report, to the extent that they engage in activities that are subject to regulation under the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

2. a financial institution, an affiliate, or a nonaffiliated third party, to the extent they engage in activities that are subject to regulation under Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and its regulations;

3. a business that collects information about a consumer if the consumer is or was (a) in a contractual relationship with the business, (b) an investor in or donor to the business, or (c) in any relationship with the business that is like the relationships above;

4. a business that performs services or acts as the agent for a business where the consumer has a previous relationship, as described above, or a governmental entity;

5. a business collecting data to regulate certain federally listed chemicals (21 U.S.C. § 830);

6. a candidate committee, national committee, party committee, or political committee; and

7. a covered entity or business associate under the Health Insurance Portability and Accountability Act (HIPAA) regulations (for example, health plans, health care clearinghouses, and health care providers).

The bill specifies that its data broker provisions do not prohibit an unregistered data broker from engaging in any sale or licensing of brokered personal data if it exclusively involves:

1. publicly available information that is (a) about a consumer's business or profession; (b) sold or licensed as part of a service that provides alerts for health or safety purposes; or (c) lawfully available from any federal, state, or local government record, unless the information is collated and combined to create a consumer profile that is made available to a user of a publicly

accessible website, or used to generate inferences related to consumers;

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

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

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

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

Data Broker Registration Account (§ 8)

The bill establishes the data broker registration account as a separate, nonlapsing account. The account must contain any money the law requires and the DCP commissioner must spend the money for the accessible deletion mechanism program.

Regulations (§ 9)

The bill allows the DCP commissioner to adopt regulations to implement these provisions.

Penalty (§ 10)

The bill allows the DCP commissioner, after giving notice and holding a hearing following the Uniform Administrative Procedure Act, to impose a civil penalty of up to $200 per day for each violation of the bill's data broker provisions. Any civil penalty collected must be deposited into the data broker registration account.

§ 11 — PRICING USING CONSUMER PERSONAL DATA

Generally requires anyone doing business in the state who uses a price setting device (automated process using a consumer's personal data to set a price) to advertise a consumer good or service online to provide a disclosure that a device was used in pricing; generally prohibits surveillance pricing (establishing a customized price for a consumer good or service that is consumer-specific based on the consumer's personal data collected)

Price Setting Device Disclosure

The bill generally requires anyone doing business in the state who uses a price setting device (any automated or programmed process that uses a consumer's personal data to set a price) and advertises or promotes a consumer good or service online with its price, to include in the online advertisement, promotion, label, statement, display, image, offer or announcement the following disclosure, or a substantially similar disclosure: "THIS PRICE WAS INCREASED BY A PRICE SETTING DEVICE USING YOUR PERSONAL DATA." This disclosure must be readily visible to the average consumer.

This requirement does not apply to those using a device to establish a discounted price for a consumer good or service for an online transaction.

Surveillance Pricing

The bill generally prohibits a retail seller or third-party delivery service doing business in the state from engaging in surveillance pricing. A "third-party delivery service" is a company, organization, or entity, outside a retail food establishment's business operation, that facilitates delivery or online ordering services to retail food establishment customers.

"Surveillance pricing" is the practice of setting a customized price for a consumer good or service that is consumer-specific based on the consumer's personal data collected:

1. through any technology or technological method, system, or tool, including any biometric monitoring, camera, device tracking, or sensor, that is capable of gathering personal data on a consumer's behavior, characteristics, location, or other personal attributes; and

2. by the person establishing the customized price by gathering, purchasing, or acquiring the personal data from a third party.

It does not include establishing for, or offering to:

1. a consumer a discounted price for a consumer service to retain the consumer as a customer;

2. different consumers different prices for the same consumer good or service due to (a) justifiable differences in the costs incurred in providing the good or service, including differences in consumer selections, delivery distances, or delivery times, or (b) justifiable temporal differences, including temporal differences due to price fluctuations based on supply and demand; or

3. a consumer or group of consumers a discounted price for a consumer good or service (a) based on publicly disclosed uniform terms and conditions that may be satisfied by any consumer, including by signing up for a mailing list, disclosing personal data, registering for promotional communications, or participating in a promotional event; (b) that is available to all consumers who are members of a broadly defined group, including veterans or armed forces members, senior citizens, students, teachers, or residents of a specific area; or (c) through a loyalty, membership, or rewards program that consumers affirmatively enroll.

For discounted prices, the retail seller or third-party delivery service must (1) prominently post the discounted price, and the uniform terms and conditions for the discounted price, on the retail seller's or third-party delivery service's website in readily understandable language for an average consumer and (2) offer the discounted price to all consumers according to the posted uniform terms and conditions.

Exemptions

The bill specifies that the price setting disclosure and surveillance pricing provisions do not apply to:

1. anyone who is or must be licensed, authorized to operate, or registered under the state's insurance laws;

2. any financial institution or its affiliate, to the extent they are subject to Title V of the federal Gramm- Leach-Bliley Act (15 U.S.C. § 6801); or

3. any bank, holding company, out-of-state bank, or out-of-state holding company, that establishes an office in the state and is subject to the Banking Commissioner's supervision or regulation.

The bill deems violations of these provisions a Connecticut Unfair Trade Practices Act (CUTPA) violation solely enforced by the attorney general (and not by a private right of action or class action).

§§ 12-17 — CTDPA

Modifies what is considered publicly available information for CTDPA purposes and allows consumers to delete certain information that is made into a profile; limits the use of facial recognition technology to matching still images or video to a database and requires certain signage, among other requirements; prohibits controllers from selling precise geolocation data

Publicly Available Information (§§ 12 & 13)

Under existing law, publicly available information is not "personal data" and is, therefore, not subject to the CTDPA (see BACKGROUND).

The bill modifies what is considered publicly available information. Under current law, as amended by PA 25-113, which will go into effect July 1, 2026, "publicly available information" is information that (1) is lawfully available through federal, state, or municipal government records or widely distributed media or (2) a controller has a reasonable basis to believe the consumer has lawfully made available to the general public or has been lawfully made available to the general public from widely distributed media.

The bill expands what is considered publicly available information:

1. by removing the requirement that governmental records be lawfully made available, and instead just requires their availability, and

2. to include all data from a widely distributed media, regardless of whether the information was made available lawfully, rather than only when the controller reasonably believes information has been lawfully made available from widely distributed media.

Current law has various exemptions to what is considered publicly available data, including biometric data that can be associated with a specific consumer and was collected without the consumer's consent. The bill instead exempts biometric data a business collects about a consumer without his or her knowledge.

The bill also adds the following exemptions:

1. obscene visual depictions;

2. personal data created by combining any personal data with any publicly available information;

3. genetic data, unless the consumer makes it publicly available;

4. information a consumer provides on a publicly accessible website or online service where the (a) website or online service is made available to the general public and (b) consumer has a reasonable expectation of privacy in the information, including by restricting the information to a specific audience; or

5. intimate images or synthetically created intimate images known to be nonconsensual, as defined under the state's unlawful dissemination of an intimate or synthetic image laws.

The bill gives a consumer the right to delete publicly available information that is (1) collated and combined to create a consumer profile that is made available to a publicly accessible website's user for compensation or for free or (2) made available for sale. This right also includes any inference generated from this information.

Facial Recognition Technology (§§ 12 & 16)

The bill requires controllers or consumer health data controllers that use facial recognition technology on their premises for certain purposes

to:

1. exclusively use the facial recognition technology to match still images or video to a database they exclusively control and

2. post clearly legible signs at each entrance where the technology is used, other than entrances where access is restricted to authorized employees.

The signs must (1) alert consumers entering the premises that facial recognition technology is being used and (2) include a conspicuous hyperlink or quick response (QR) code that directs consumers to the facial recognition technology policy the controller or consumer health data controller maintains. This policy must include contact information for the attorney general's office and may disclose the controller's or consumer health data controller's policies on interactions between their loss prevention officers and consumers.

The controller or data controller must use the facial recognition technology only to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for these actions.

Precise Geolocation (§§ 14 & 15)

The bill generally prohibits controllers and third parties from selling a consumer's precise geolocation data. This does not apply to communications content, or any data generated by or connected to advanced utility metering infrastructure systems or equipment a utility uses.

Under existing law, certain controllers are generally prohibited from collecting a minor's precise geolocation and must, when collecting this data, give the minor a signal that the collection is happening. It is also considered sensitive data that a controller may not process without consumer consent or, if the consumer is younger than age 13, the minor's parent or guardian's consent.

§§ 17-19 — DIRECT-TO-CONSUMER GENETIC TESTING

Gives consumers a property right and exclusive control over their biological samples that are given to a direct-to-consumer genetic testing company and their results; requires these companies to disclose certain policies and procedures to consumers and get a consumer's consent for various uses of their genetic data; deems violations as CUTPA violations

The bill gives consumers a property right and exclusive control over:

1. their biological samples (material from a person's body known to contain DNA including tissue, blood, urine, and saliva) that are given to or used by a direct-to-consumer genetic testing company and

2. results from genetic testing by these companies on their DNA.

This includes the right of control over the collection, use, retention, maintenance, disclosure, and destruction of a consumer's biological sample and results. The bill requires direct-to-consumer genetic testing companies to conduct their business and affairs consistent with these rights.

Additionally, the bill requires these companies to (1) disclose certain policies and procedures to consumers and (2) get a consumer's consent for various uses of their genetic data. The bill prohibits companies from disclosing the results of genetic testing on a consumer's DNA to anyone other than the consumer unless the consumer expressly consents to the disclosure, or it is disclosed to someone under a court order, warrant, or subpoena.

The bill also requires companies to have security procedures and certain processes to let consumers take certain actions.

Under the bill, violations of the bill's genetic testing provisions are deemed a CUTPA violation solely enforced by the attorney general (and not by a private right of action or class action).

Scope of the Bill

Direct-to-Consumer Genetic Testing Companies. The bill applies to "direct-to-consumer genetic testing companies," which are individuals or entities that, in the ordinary course of business in

Connecticut, offer genetic testing directly to a consumer or collect, use, or analyze genetic data given by a consumer. These are not licensed health care services providers who, within the scope of their practice, order genetic testing for a medical purpose.

Genetic Testing. Under the bill, "genetic testing" is (1) a lab test of a person's complete DNA sequence or a DNA region, chromosome, gene, or gene product to determine the presence or absence of a genetic characteristic and (2) an interpretation of genetic data.

Genetic Data. "Genetic data" is data in any format about an individual's genetic characteristics. It includes:

1. raw sequence data that results from sequencing all or part of a person's DNA;

2. genotypic (a person's unique sequence of DNA) or phenotypic (a person's observable characteristics) information from analyzing raw sequence data; and

3. information that (a) is about a person's health condition, (b) the person gives the company, or (c) the company analyzes related to raw sequence data and uses for scientific research or product development.

It does not include de-identified data, which is data that cannot reasonably be used to infer information about, or be linked to, an individual as long as the company that has the data (1) takes administrative and technical steps to make sure it cannot be associated with an individual, (2) publicly commits to have and use it only in de-identified form and does not re-identify it, and (3) contractually obligates any recipient of the data to do the same.

Policy Disclosures

The bill requires companies to:

1. disclose their policies and procedures on the collection, use, and disclosure of genetic data before taking a consumer's biological

sample, genetic data, or payment; and

2. prominently display a privacy notice on their websites with their policies and procedures on the collection, use, access, disclosure, transfer, security, retention, and deletion of a consumer's data and consent.

Consent Requirements

Collecting, Using, or Disclosing Genetic Data. The bill requires companies to get a consumer's express consent to collect, use, or disclose the consumer's genetic data. Before doing so, companies must disclose to the consumer:

1. their policies and procedures on using consumers' genetic data they collect;

2. each person who may access the results of genetic testing they perform, including vendors or service providers; and

3. how the company may disclose the consumer's genetic data.

Express consent under the bill requires the consumer to affirmatively respond to a clear, meaningful, and prominent notice about collecting, using, retaining, or disclosing the consumer's genetic data for a specific purpose.

Transferring Genetic Data, Using It for Other Purposes, and Retaining Samples. The bill requires a company to get a separate express consent before:

1. disclosing or transferring genetic data to anyone other than a vendor or service provider,

2. using the genetic data for any purpose other than the primary purpose the company gave to the consumer, or

3. retaining a consumer's biological sample after completing genetic testing.

Research Purposes. The bill requires a company to get the consumer's informed consent in compliance with federal regulations on human subjects to disclose or transfer genetic data to a third party for research purposes or research done under the company's control for publication or generalized knowledge.

Prohibited Disclosures

The bill prohibits a company from disclosing a consumer's genetic data to:

1. the consumer's employer;

2. someone who in the ordinary course of business offers health, life, or long-term care insurance or provides information to an insurer, health care center, or fraternal benefit society for underwriting or rating risks; or

3. a third party the company knows or reasonably should know intends to use it for marketing, including targeted advertising.

Security and Company Procedures

The bill requires companies to have reasonable security measures to protect consumers' biological samples and genetic data from unauthorized access, destruction, use, modification, or disclosure. It also requires companies to have procedures that allow consumers to:

1. access their genetic data;

2. require the company to delete their genetic data or destroy, and confirm destruction of, their biological samples; and

3. revoke consent for using their genetic data for research, including by a third party.

§ 20 — ADVERTISEMENT VOLUME WHEN STREAMING

Prohibits a streaming video service from transmitting to a consumer commercial advertising audio that is louder than the video it accompanies, consistent with FCC regulations; makes violations a CUTPA violation

Beginning January 1, 2027, the bill prohibits a streaming video service

from transmitting to a consumer the audio of commercial advertising with a volume that is louder than the video content that accompanies the commercial advertisement, consistent with the Federal Communications Commission (FCC) regulations for television broadcasts or multichannel video programming distributers (such as cable operators or satellite providers who provide multiple channels of video programs to subscribers or customers) (see *FCC Regulations* below).

The bill makes violations of its streaming provisions a CUTPA violation solely enforced by the attorney general (and not by a private right of action or class action).

BACKGROUND

CTDPA

The CTDPA, among other things:

1. sets a framework for controlling and processing personal data,

2. sets responsibilities and privacy protection standards for data controllers (those that determine the purpose and means of processing personal data) and processors (those that process data for a controller), and

3. generally applies to individuals (1) doing business in Connecticut or producing products or services targeted to state residents and (2) controlling or processing personal data of numbers of consumers above specified thresholds during the previous calendar year.

FCC Regulations

FCC regulations generally require television stations, cable operators, satellite providers, and certain others to have commercial advertising at a similar volume to the programming it accompanies. It deems a provider in compliance when using certain equipment and methods and includes various safe harbor provisions (47 C.F.R. §§ 73.682 & 76.607).

In February 2025, the FCC began a rulemaking process to consider

updating its commercial loudness rules, including whether to apply them to streaming platforms (FCC-25-16, Docket No. 25-72).

Related Bills

sSB 232 (File 217), favorably reported by the General Law Committee, has similar provisions on streaming video services and the volume of commercial advertisements.

sHB 5128 (File 233), favorably reported by the General Law Committee, has substantially similar provisions on direct-to-consumer genetic testing.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 16 Nay 5 (03/16/2026)

Judiciary Committee

Joint Favorable
Yea 31 Nay 9 (04/10/2026)

Appropriations Committee

Joint Favorable
Yea 40 Nay 13 (04/17/2026)