OLR Bill Analysis

sSB 3 (File 604, as amended by Senate "A")*

AN ACT CONCERNING ONLINE PRIVACY, DATA AND SAFETY PROTECTIONS.

SUMMARY

This bill sets standards on accessing and sharing consumer health data by certain private entities that do business in Connecticut (§§ 1 & 2). For example, the bill generally prohibits these parties from (1) selling this data without the consumer's consent or (2) using a "geofence" to create a virtual boundary near mental health or reproductive or sexual health facilities to collect consumer health data. It also places various specific limitations on "consumer health data controllers" (i.e., people or entities that determine the purposes and means of processing consumer health data). It incorporates various provisions on consumer health data controllers into the existing law (set to take effect this July) on consumer data privacy and online monitoring and makes other changes to the existing data privacy law (§§ 3-6).

The bill's provisions on consumer health data and consumer health data controllers generally apply to individuals or entities that (1) conduct business in Connecticut or (2) produce products or services that are targeted to Connecticut residents. By contrast, the existing data privacy law exempts individuals or entities whose actions do not meet a specified threshold number of consumers or percentage of related gross revenue.

The bill 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 of receiving an authenticated request (§ 7).

Additionally, the bill also establishes a framework and sets requirements for how individuals or entities offering certain online services, products, and features manage and process personal data for

minors (i.e., those under age 18) (§§ 8-13). It specifically requires them to use reasonable care to avoid having their services, products, and features cause, any heightened risk of harm to a minor. They are also prohibited from (1) processing the minor's personal data without receiving the minor's or his or her parent's or guardian's consent, (2) using any system design feature to significantly increase, sustain, or extend a minor's use of such online service, product, or feature, and (3) collecting a minor's precise geolocation data.

Under the bill, any violation of the consumer health data, social media, online services provisions is deemed a violation under the Connecticut Unfair Trade Practices Act (CUTPA), enforced solely by the attorney general (§§ 6, 7 & 13). It further specifies that none of its provisions may be construed to create a private right of action or grounds for a class action under CUTPA.

The bill also:

1. requires online dating operators to adopt a policy for handling harassment reports by or between users and to maintain an online safety center to provide users with resources on safe dating (§§ 14-16); and

2. statutorily establishes the Connecticut Internet Crimes Against Children task force (CT ICAC) and requires it to use state and federal funding appropriated to it in a way that is consistent with its duties under federal law (§ 17).

*Senate Amendment "A" (1) moves up the effective dates for the provisions on consumer health data and minors and online services, and delays the effective date for the online dating provision; (2) makes various changes to the consumer health data provisions and existing data privacy law, such as incorporating consumer health data controllers into the existing law and removing provisions from the underlying bill on a specific consent form for selling consumer health data; (3) eliminates the underlying bill's prohibition on social media platforms establishing an account for a minor under age 16 without a parent's or guardian's consent; (4) increases the time a social media

platform has to delete a minor's account; (5) makes various minor changes to the minors and online services provisions; (6) eliminates the provision in the underlying bill allowing courts to order certain computer and communication services not to disclose certain records; and (7) requires online dating operators to adopt a policy for handling harassment reports and maintain an online safety center rather than requiring them to owe a duty of care to users to protect them against potential criminal activity of other users.

EFFECTIVE DATE: July 1, 2023, except the online dating provisions are effective January 1, 2024, the social media provision is effective July 1, 2024, and the minors and online services provisions are effective October 1, 2024.

§ 1 — CONSUMER HEALTH DATA DEFINITIONS

Consumer Health Data Generally

For purposes of the bill, "consumer health data" is any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, including gender-affirming and reproductive or sexual health data.

As under the existing consumer data privacy and online monitoring law (see BACKGROUND), a "consumer" for these purposes is a state resident, excluding anyone acting (1) in a commercial or employment context or (2) as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the controller occur solely within the context of that person's role with the entity.

As under existing law, a "controller" is a person (individual or legal entity) who, alone or jointly with others, determines the purpose and means of processing "personal data" (i.e., any information that is linked, or reasonably linkable, to an identified or identifiable individual, excluding de-identified data or publicly available information). Under the bill, a "consumer health data controller" is a controller that, alone or jointly with others, determines the purpose and means of processing consumer health data.

Gender-Affirming Health Data

Under the bill, "gender-affirming health data" is any personal data about a consumer's efforts to seek, or receiving, gender-affirming health care services (i.e., all medical care related to treatments for gender dysphoria).

Reproductive or Sexual Health Data

For the purposes of the bill, "reproductive or sexual health data" is any personal data about a consumer's effort to seek, or receiving, reproductive or sexual health care.

"Reproductive or sexual health care" is any health service or product that concerns a consumer's reproductive system or sexual well-being, including any that concern the following:

1. an individual health condition, status, disease, diagnosis, diagnostic test, or treatment;

2. a social, psychological, behavioral, or medical intervention;

3. a surgery or procedure, including an abortion;

4. medication use or purchase, including for the purposes of an abortion;

5. a bodily function, vital sign, or symptom (or measurement of any of them); or

6. an abortion, including related medical or nonmedical services, products, diagnostics, counseling, or follow-up services.

§§ 2 & 3 — CONSUMER HEALTH DATA MANAGEMENT

Subject to various exemptions (see EXEMPTIONS FROM DATA PRIVACY LAWS below), the bill prohibits the following actions relating to consumer health data.

Consumer Health Data Access and Security (§ 2(a)(1)(A) & (B))

The bill generally prohibits anyone from providing any employee or

contractor with access to consumer health data unless the employee or contractor is subject to a contractual or statutory duty of confidentiality.

It also generally prohibits anyone from providing a processor with access to consumer health data unless the person and processor comply with specified existing requirements, such as that (1) the processor adheres to the controller's instructions and (2) a contract between the controller and processor governs the processor's data processing procedures for processing performed on the controller's behalf. By law, among various other elements, these contracts must require the processor to (1) ensure that each person processing personal data is subject to a duty of confidentiality regarding it and (2) at the controller's direction, delete or return all personal data to the controller as requested at the end of providing services unless the law requires that it be retained (CGS § 42-521).

As under existing law, "processors" are those who process "personal data" for a "controller" (see above).

Prohibition on Using Geofences (§ 2(a)(1)(C))

The bill generally prohibits anyone from using a geofence to set a virtual boundary within 1,750 feet of any mental health facility or reproductive or sexual health facility to identify, track, collect data from, or send notifications to consumers about their consumer health data.

Under the bill, a "geofence" is any technology that uses global positioning coordinates (i.e., GPS), cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data, or any other form of location detection, or any combination of them to establish a virtual boundary.

A "mental health facility" is any health care facility in which at least 70% of its health care services are mental health services. A "reproductive or sexual health facility" is any health care facility in which at least 70% of its health care-related services or products are for reproductive or sexual health care.

Prohibition on Selling Consumer Health Data Without Consent (§ 2(a)(1)(D))

The bill generally prohibits anyone from selling, or offering to sell, consumer health data without first getting the consumer's consent.

Under existing law, "consent" is a clear affirmative act signifying the consumer's specific informed agreement to allow the processing of his or her personal data, including by written statement, which may be electronic. It does not include (1) accepting a general or broad terms of use or similar document that contains personal data processing descriptions along with other, unrelated information; (2) hovering over, muting, pausing, or closing a given piece of content; or (3) obtaining agreement through the use of dark patterns. A "dark pattern" (1) is a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice and (2) includes any practice the Federal Trade Commission refers to as a "dark pattern."

§§ 2 & 3 — EXEMPTIONS FROM DATA PRIVACY LAWS

The bill's provisions on consumer health data and consumer health data controllers generally apply to all individuals or entities that (1) conduct business in Connecticut or (2) produce products or services that are targeted to Connecticut residents.

But as under the state's existing consumer data privacy and online monitoring law (see § 3), the bill's provisions on consumer health data do not apply to certain entities, including the following:

1. state bodies, authorities, boards, bureaus, commissions, districts, or agencies or those of its political subdivisions;

2. higher education institutions;

3. national securities associations registered under federal law;

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

5. covered entities or business associates, as defined in federal

Health Insurance Portability and Accountability Act (HIPAA) regulations (e.g., health plans, health care clearinghouses, and health care providers).

The bill also exempts the following from its consumer health data provisions and the existing consumer data privacy and online monitoring law:

1. anyone who has entered into a contract with a state or local body, authority, or similar entity (see the first item in the list above) to process consumer health data on the entity's behalf;

2. tribal nation government organizations; and

3. air carriers (i.e., U.S. citizens that provide air transportation by any means) that are regulated under the Federal Aviation Act of 1958 (49 U.S.C. § 40101 et seq.) and the Airline Deregulation Act (49 U.S.C. § 41713).

The existing law also exempts federally tax-exempt nonprofit organizations. The bill does not extend this exemption to consumer health data.

As under the consumer data privacy and online monitoring law, the bill also exempts certain information and data. This includes the following:

1. protected health information under HIPAA (42 U.S.C. § 1320d et seq.);

2. patient-identifying information under a federal law on substance use disorder treatment (42 U.S.C. § 290dd-2);

3. identifiable private information under the federal policy for protecting human subjects (45 C.F.R. Part 46);

4. identifiable private information collected as part of human subject research under the good clinical practice guidelines issued by the International Council for Harmonization of

Technical Requirements for Pharmaceuticals for Human Use;

5. information and data related to protecting human subjects (21 C.F.R. Parts 6, 50, and 56) or personal data used or shared in research done following the standards for protecting human subjects the bill exempts above, or other research done following applicable law (45 C.F.R. § 164.501);

6. information and documents created for the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. § 11101 et seq.);

7. patient safety work product for patient safety organizations under state law (CGS § 19a-127o) and the federal Patient Safety and Quality Improvement Act (42 U.S.C. § 299b-21 et seq.);

8. information derived from any health care-related information listed in the information or data exemption list that is de-identified according to HIPAA's de-identification requirements;

9. information originating from and intermingled to be indistinguishable with, or treated in the same way as, other exempt information under the bill maintained by a covered entity (e.g., health care providers and plans) or business associate, program, or qualified service organization, as specified in a federal law on substance use disorder treatment (42 U.S.C. § 290dd-2);

10. information used for public health activities and purposes as authorized by HIPAA, community health activities, and population health activities;

11. the collection, maintenance, disclosure, sale, communication, or use of any personal information relating to a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that activity is regulated

by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

12. personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

13. personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g et seq.);

14. personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.);

15. data processed or maintained (a) in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party (or consumer health data controller under the bill), to the extent that the data is collected and used within the context of that role; (b) as an individual's emergency contact information and used for emergency contact purposes; or (c) that must be retained to administer benefits for another individual whose data is HIPAA-protected; and

16. personal data collected, processed, sold, or disclosed in relation to price, route, or service, as used under specified federal aviation-related laws.

Parental Consent Exemption (§ 3(c))

The existing consumer data privacy and online monitoring law deems controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act (COPPA) (15 U.S.C. § 6501 et seq.) compliant with any obligation to obtain parental consent under the law.

The bill extends this exemption to consumer health data controllers the comply with COPPA's verifiable parent consent requirements.

§ 5 — PROCESSING PERSONAL DATA FOR SPECIFIED PURPOSES

The bill specifically extends several existing provisions of the consumer data privacy and online monitoring law to apply to consumer health data controllers, as follows.

Ability to Comply With or Take Certain Other Actions (§ 5(a))

As under existing law for controllers or processors, the bill specifies that nothing under the bill's health data requirements (see § 2 above) or existing law should be construed to restrict a consumer health data controller's ability to:

1. comply with federal, state, or municipal ordinances or regulations, or a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other governmental authorities;

2. cooperate with law enforcement agencies concerning conduct or activity that the consumer health data controller reasonably and in good faith believes may violate federal, state, or municipal ordinances or regulations;

3. investigate, establish, exercise, prepare for, or defend legal claims;

4. provide a product or service a consumer specifically requested;

5. perform a contract to which a consumer is a party, including by fulfilling written warranty terms;

6. take steps at the consumer's request before entering into a contract;

7. take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or an individual and where the processing cannot be manifestly based on another legal basis;

8. 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;

9. engage in public- or peer-reviewed scientific or statistical research in the public interest that follows applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines, or similar independent oversight entities that determine, whether (a) deleting the information is likely to provide substantial benefits that do not exclusively benefit the consumer health data controller, (b) the research's expected benefits outweigh the privacy risk, and (c) the consumer health data controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

10. assist another controller, processor, or third party with any obligations under the bill or existing law; or

11. process personal data for reasons of public interest in public health, community health, or population health, but solely to the extent that the processing is (a) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed and (b) under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

Ability to Collect, Use, or Retain Data (§ 5(b))

As under existing law for controllers or processors, the bill also specifies that the obligations existing law and the bill impose on consumer health data controllers do not restrict their ability to collect, use, or retain data for internal use to:

1. conduct internal research to develop, improve, or repair products, services, or technology;

2. recall products;

3. identify and repair technical errors that impair existing or intended functionality; or

4. perform internal operations that are reasonably aligned with the consumer's expectations, reasonably anticipated based on the consumer's existing relationship with the consumer health data controller, or compatible with processing data based on (a) providing a product or service the consumer specifically requested or (b) performing a contract to which the consumer is a party.

Evidentiary Privilege (§ 5(c))

Under the bill, as under existing law for controllers or processors, the bill's or law's obligations imposed on consumer health data controllers do not apply if doing so would make them violate a state evidentiary privilege. The bill and existing law should not be construed to prevent a consumer health data controller from providing personal data about a consumer to a person covered by state evidentiary privilege laws as a privileged communication.

Third-Party Liability (§ 5(d))

Under the bill, as under existing law for controllers or processors, consumer health data controllers that disclose personal data to a processor or third-party controller under the bill's or law's requirements are not responsible for violations by them.

At the time of disclosure, the original consumer health data controller must not have had actual knowledge that the recipient would violate the bill or law. A third-party controller or processor receiving personal data from a consumer health data controller in compliance with the bill and law is also not in violation for that controller's transgressions.

First Amendment Rights (§ 5(e))

As under existing law for controllers and processors, the bill states that the bill's and existing law's provisions are not to be construed to: (1) impose an obligation on a consumer health data controller that adversely affects the rights and freedoms of any person, including his

or her rights to free speech or freedom of the press guaranteed under the First Amendment of the U.S. Constitution or the state law protecting disclosure of information by news media (CGS § 52-146t). It also does not affect a person processing personal data for a purely personal or household activity.

Limitations on Processing Personal Data (§ 5(f) & (g))

Under the bill (as under existing law for controllers), consumer health data controllers may process data to the extent the processing is (1) reasonably necessary and proportionate to the purposes listed above (e.g., for internal research or product recall) and (2) adequate, relevant, and limited to what is needed for the specific listed purpose. When applicable, personal data collected, used, or retained must consider the nature and purposes of these actions. The data must be subject to reasonable administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to consumers related to its collection, use, or retention.

As under existing law for controllers, if a consumer health data controller processes personal data for a specified purpose through one of the exemptions listed above, that party bears the burden of showing that the processing (1) qualifies for an exemption and (2) complies with the requirements for processing personal data (see above).

Controller Determination (§ 5 (h))

The bill specifies that processing personal data for the purposes expressly identified in this provision does not, on its own, make an entity a consumer health data controller (or a controller under existing law).

§ 6 — ATTORNEY GENERAL'S POWERS

The bill extends existing law's enforcement provisions to its new provisions on consumer health data controllers. Under these provisions:

1. the attorney general has exclusive authority to enforce violations;

2. there is a grace period through December 31, 2024, during which

the attorney general must give violators an opportunity to cure any violations;

3. starting January 1, 2025, the attorney general has discretion over whether to provide an opportunity to correct an alleged violation;

4. the bill's provisions should not be construed as providing the basis for, or be subject to, a private right of action for violations under the bill or any other law; and

5. any violation of the bill's requirements is a CUTPA violation and is enforced solely by the attorney general, but CUTPA's private right of action and class action provisions do not apply to the violation.

Notice of and Opportunity to Correct Violations

From July 1, 2023, to December 31, 2024, the bill, as under existing law, requires the attorney general, before initiating any action for a violation of its provisions, to issue a notice of violation to the consumer health data controller if he determines a cure is possible. If the controller fails to cure the violation within 60 days after receiving notice, the attorney general may bring an action.

Under existing law, by February 1, 2024, the attorney general must submit a report to the General Law Committee disclosing specified related information.

Violations After January 1, 2025

As under existing law for controllers or processors, beginning on January 1, 2025, the attorney general may, in determining whether to give a consumer health data controller the opportunity to cure an alleged violation, consider:

1. the number of violations,

2. the consumer health data controller's complexity and the nature and extent of their processing activities,

3. the substantial likelihood of injury to the public,

4. the safety of individuals or property, and

5. whether the alleged violation was likely caused by human or technical error.

OTHER CHANGES TO EXISTING DATA PRIVACY AND ONLINE MONITORING LAW

Specific Restrictions on Sensitive Data (§ 1)

Existing law prohibits controllers from processing sensitive data about the consumer without consent, or if the consumer is a known child (i.e., younger than age 13), without processing the data in accordance with COPPA. 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 processing sensitive data.

The bill expands the definition of "sensitive data" for these purposes to cover personal data that includes (1) consumer health data or (2) data about someone's status as a crime victim. Under existing law, a crime victim is someone who suffers direct or threatened physical, emotional, or financial harm because of a crime and includes (1) immediate family members of a minor, incompetent individual, or homicide victim and (2) a homicide victim's designated decision maker (CGS §§ 1-1k & 1-56r).

Under existing law, "sensitive data" is personal data that includes (1) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status; (2) processing genetic or biometric data in order to uniquely identify an individual; (3) personal data collected from a known child; or (4) precise geolocation data.

Prohibition on Certain Actions as to Minors (§ 4)

Existing law prohibits controllers from processing a consumer's personal data for purposes of targeted advertising, or selling the consumer's data, without the consumer's consent for consumers who

are at least 13 years old, but under 16 years old. Under current law, for the prohibition to apply, the controller must have actual knowledge that the consumer's age is in this range and willfully disregard it. Under the bill, either actual knowledge or willful disregard of the consumer's age makes a controller subject to the prohibition.

§ 7 — UNPUBLISHING MINORS' SOCIAL MEDIA ACCOUNTS

Requests to Unpublish

The bill requires a social media platform that receives a request from a minor, or the minor's parent or legal guardian if the minor is under age 16, to unpublish (i.e., remove a social media platform account from public visibility) the minor's account within 15 business days of receiving the request.

Under the bill, "social media platform" means 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 such service or application, and

3. enables a user to (a) construct a public or semi-public profile for the purposes of signing into and using such service or application, (b) populate a public list of other users with whom the user shares a social connection within such service or application, and (c) create or post content that is viewable by other users, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users.

"Social media platform" does not include a public or semi-public Internet-based service or application that:

1. exclusively provides e-mail or direct messaging services;

2. primarily consists of news, sports, entertainment, interactive video games, electronic commerce, or content preselected by the

provider or for which any chat, comments, or interactive functionality is incidental to, 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 a student engagement program.

Deletion

The bill also requires a social media platform, within 45 business days after receiving such request, to delete the social media platform account. The platform must delete the account and cease processing the minor's personal data except where the preservation of the account or personal data is otherwise permitted or required by law. A platform may extend this period by another 45 business days if the extension is reasonably needed when considering the complexity and number of consumer requests. The platform must inform the person making the request within the initial 45 business days of the extension and reason for it.

Privacy Notice

The bill requires a social media platform to establish and describe in a privacy notice, one or more secure and reliable means for submitting a request to unpublish. A platform that provides a mechanism to initiate a process to delete or unpublish a minor's social media platform is deemed in compliance with this requirement.

Unable to Authenticate

Under the bill, a platform is not required to comply with a request that it is unable to authenticate. But the platform must provide a notice to the consumer who submitted the request stating that it is unable to authenticate the request and will not be able to authenticate until the consumer provides additional reasonably necessary information. Under the bill, "authenticate" means to use reasonable means and make a commercially reasonable effort to determine whether a request to unpublish data, was made by or on behalf of, the minor with the right to make the request.

Violations

Under the bill, a violation of the social media account provisions is a CUTPA violation and can be enforced solely by the attorney general. CUTPA's private right of action and class action provisions do not apply to these violations.

§§ 8-13 — MINORS AND ONLINE SERVICES, PRODUCTS, AND FEATURES

The bill also establishes a framework and sets requirements for how controllers who offer online services, products, and services manage, process, and get consent to use the personal data of "minors" (i.e., consumers under age 18). Under the bill, "online service, product, or feature" is any service, product, or feature that is provided online, but excludes any (1) telecommunications service, (2) broadband Internet access service, or (3) delivery or use of a physical product. "Controllers," "process," "consent," "personal data," and "consumers" have the same meanings as in the data privacy and online monitoring law (see § 1).

Avoiding Heightened Risk of Harm to Minors (§ 9(a))

If a controller offers an online service, product, or feature to consumers whom it has actual knowledge, or willfully disregards, are minors, the bill requires the controller to use reasonable care to avoid having their online service, product, or feature cause any heightened risk of harm to minors.

Under the bill, "heightened risk of harm to minors" is processing minors' personal data, including in a way that presents any reasonably 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 a minor's solitude, seclusion, private affairs, or concerns, if a reasonable person would be offended by the intrusion.

Collecting Minors' Precise Geolocation Data and Processing Minors' Personal Data (§ 9(b))

If a controller offers an online service, product, or feature to consumers who it has actual knowledge, or willfully disregards, are minors, the bill generally prohibits the controller from (1) collecting minors' precise geolocation data or processing their personal data (see below) or (2) using any system design feature to significantly increase, sustain, or extend their 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. A controller that complies with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) is deemed to have satisfied the bill's consent requirement.

Specifically, the bill prohibits these controllers from collecting a minor's precise geolocation data unless (1) the data is reasonably needed for the controller to provide the online service, product, or feature and, if so, the controller may only collect the data for the time needed to do that; and (2) the controller gives the minor a signal indicating that it is collecting the data, with the signal being available to the minor for the entire time.

The bill specifically prohibits these controllers from processing any minor's personal data:

1. for the purposes of (a) targeted advertising, (b) any sale of personal data, or (c) profiling to further any fully automated decision the controller makes that produces any legal or similarly significant effect in the controller providing or denying any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care services, or access to essential goods or services;

2. unless the processing is reasonably necessary to provide the online service, product, or feature;

3. for any processing purpose other than as disclosed at the time the

controller collected the personal data or that is reasonably necessary for, and compatible with, these processing purposes;

4. for longer than is reasonably necessary to provide the online service, product, or feature; or

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

Other than the prohibition on collecting geolocation data, these prohibitions do not apply to any service or application that is used by and under the direction of an educational entity, including a learning management system or a student engagement program.

Under the bill, "targeted advertising" means displaying specific advertisements to a consumer based on personal data obtained or inferred from his or her activities over time and across nonaffiliated websites or online applications to predict preferences or interests. It excludes:

1. advertisements based on activities within a controller's own websites or online applications;

2. advertisements based on the context of a consumer's current search query, website visit, or online application;

3. advertisements directed to a consumer in response to his or her request for information or feedback; or

4. processing personal data solely measuring or reporting advertising frequency, performance, or reach.

"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 (CGS § 42-515(22)).

"Sale of personal data" is the exchange of personal data for monetary or other valuable consideration by the controller to a "third party" (an individual or legal entity other than the consumer or controller or processor or their affiliate). It excludes the following:

1. disclosing personal data (a) to a processor that processes it on the controller's behalf, (b) to a third party for providing a product or service the consumer requested, or (c) where the consumer directs the controller to disclose the data or intentionally uses the controller to interact with a third party;

2. disclosing or transferring personal data to (a) the controller's affiliate or (b) a third party as an asset that is part of an actual or proposed merger, acquisition, bankruptcy, or other transaction where the third party assumes control of all or part of the controller's assets; and

3. disclosing personal data that the consumer (a) intentionally made available to the general public through mass media and (b) did not restrict to a specific audience (CGS § 42-515(26)).

Interface Prohibitions (§ 9(c))

If a controller offers an online service, product, or feature to consumers who it has actual knowledge, or willfully disregards, are minors, the bill also prohibits it from:

1. providing any consent mechanism that is designed to substantially subvert or impair, or is manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice; or

2. offering any direct messaging apparatus for a minor to use without providing readily accessible and easy-to-use safeguards to limit an adult's ability to send unsolicited communications to minors with whom they are not connected.

These prohibitions on direct messaging apparatuses do not apply to services where the predominant or exclusive function is e-mail or direct

messaging consisting of text, photos, or videos that are sent between devices by electronic means where the messages are (1) shared between the sender and the recipient, (2) only visible to the sender and the recipient, and (3) not posted publicly.

Data Protection Assessment (§ 10)

The bill requires each controller that, on or after October 1, 2024, offers any online service, product, or feature to consumers who it has actual knowledge, or willfully disregards, are minors to do a data protection assessment of its online service, product, or feature. The assessment must be done consistently with the requirements for assessments under the state's consumer data privacy and online monitoring law (CGS § 42-522).

The assessment must also address:

1. the purpose of the online service, product, or feature;
2. the categories of minors' personal data that the online service, product, or feature processes;
3. the purposes for which the controller processes minors' personal data with respect to the online service, product, or feature; and
4. any heightened risk of harm to minors that is a reasonably foreseeable result of offering the online service, product, or feature to minors**.**

Under the bill, each controller that does a data protection assessment must: (1) review the assessment as needed to account for any material change to the processing operation of the online service, product, or feature that is subject to the assessment and (2) maintain documentation on the assessment for the longer of (a) the three-year period beginning when the processing operation ceases, or (b) as long as the controller offers the online service, product, or feature.

The bill allows a single data protection assessment to address a comparable set of processing operations that include similar activities.

And if a controller conducts an assessment to comply with another law or regulation, that assessment is deemed to satisfy the bill's assessment requirement if the assessment is reasonably similar in scope and effect to the required assessment.

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

Under the bill, data protection assessments are confidential and exempt from disclosure under the Freedom of Information Act. If any information in an assessment is disclosed to the attorney general and includes information subject to the attorney-client privilege or work product protection, the disclosure does not constitute a waiver of the privilege or protection.

Processors' Duties and Contracts With Controllers (§ 11)

The bill requires processors to adhere to the controller's instructions and (1) help them meet their obligations under the bill, and (2) provide the needed information for controllers to do data protection assessments.

Contract. The bill applies the same contract requirements that apply under the consumer data privacy and online monitoring law to processors and controllers subject to the bill's provisions on minors. Thus, the bill requires contracts to govern the processor's data processing procedures for processing done on the controller's behalf. The contract must be binding and have clear instructions for processing data, the processing's nature, purpose, and duration, and both parties' rights and obligations.

The contract must also require the processor to do the following:

1. ensure that each person processing personal data is subject to a duty of confidentiality regarding the data;

2. at the controller's direction, delete or return all personal data to

the controller as requested at the end of providing services unless the law requires that it be kept;

3. upon the controller's reasonable request, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations under the bill;

4. after giving the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the processor's obligations on personal data; and

5. either (a) allow, and cooperate with, the controller or the controller's designated assessor to make reasonable assessments or (b) arrange for a qualified and independent assessor to do so, as described below.

Under the bill, the independent assessor must evaluate the processor's policies and technical and organizational measures regarding the bill's requirements, using an appropriate and accepted control standard or framework and assessment procedure for these assessments. The processor must give a report of the assessment to the controller on request.

The bill specifies that these requirements should not be construed as relieving a controller or a processor from liability based on its role in the processing relationship.

Fact-Based Determination for Controller. Under the bill, determining whether a person is acting as a controller or processor for a specific data process is a fact-based determination that depends on the context in which the data is processed. A person that is not limited in processing personal data under a controller's instructions, or that fails to adhere to these instructions, is a controller and not a processor for that specific data processing. A processor that continues to adhere to a controller's instructions with a specific data processing remains a processor. If a processor begins, alone or with others, determining the

purposes and means of the personal data processing, the processor is a controller for that processing and may be subject to the bill's enforcement actions.

Exemptions and Construction of Controllers' and Processors' Duties (§ 12)

Exemptions. Substantially similar to the state's existing consumer data privacy and online monitoring law, the bill exempts certain entities, information, and data. (see CGS § 42-517, as amended by the bill, see § 3 above, except for the bill's provisions on minors do not exempt those who contract with governmental entities).

Ability to Comply With or Take Certain Actions. Substantially similar to the consumer data privacy and online monitoring law, the bill's online services provisions should not be construed to restrict a controller's ability to take certain actions (see CGS § 42-524, as amended by the bill, see § 5(a) above, except for items 5-7).

As under the consumer data privacy and online monitoring law (CGS § 42-524, as amended by the bill), the bill also specifies that its obligations that it imposes on controllers and processors do not:

1. restrict their ability to collect, use, or retain data for internal use (see § 5(b) above) and

2. apply if doing so would make them violate state evidentiary privilege (see § 5(c) above).

The bill also states that it should not be construed to impose an obligation on a controller or processor that adversely affects the rights and freedoms of any person, including his or her rights to free speech or freedom of the press guaranteed under the First Amendment of the U.S. Constitution or the state law protecting disclosure of information by news media (CGS § 52-146t, as amended by the bill, see § 5(e) above).

Finally, the bill allows controllers to limit the processing of personal data under certain conditions and places the burden on controller to show that the processing qualifies for an exemption and is compliant

(see § 5(f) & (g) above).

Violations (§§ 9 &13)

For any enforcement action the attorney general brings, the bill creates a rebuttable presumption that a controller used reasonable care if it complied with the provisions concerning data protection assessments.

From October 1, 2024, to December 31, 2025, the bill allows the attorney general, before initiating any enforcement action or disclosing an alleged violation of the bill's online services provisions, to issue, on a form he prescribes, a written notice of violation to a controller or processor to give it an opportunity to cure the violation.

Within 30 days of getting this notice, the controller or processor may send notice, on a form the attorney general prescribes, to the attorney general disclosing that it has (1) determined that the controller or processor did not commit the alleged violation or (2) cured the violation and taken sufficient measures to prevent further violations. If the attorney general receives a responding notice and determines that the controller or processor did not commit the alleged violation or has cured it and taken measures to prevent further violations, then the controller or processor will not be liable for any CUTPA civil penalties.

Under the bill, by February 1, 2026, the attorney general must submit a report to the General Law Committee disclosing:

1. the number of notices of violations he issued,
2. the number of violations cured within the 30-day period, and
3. any other matters he deems relevant.

Beginning on January 1, 2026, the attorney general may, in determining whether to give a controller or processor the opportunity to cure an alleged violation, consider:

1. the number of violations,

2. the controller's or processor's size and complexity and the nature and extent of their processing activities,

3. the substantial likelihood of injury to the public,

4. the safety of individuals or property,

5. whether the alleged violation was likely caused by human or technical error, and

6. the data's sensitivity.

§§ 14-16 — ONLINE DATING OPERATORS

Required Policies and Online Safety Center

The bill requires each online dating operator that offers services to Connecticut users to (1) adopt a policy for the platform's handling of harassment reports by or between users and (2) maintain an online safety center that is reasonably designed to provide users with resources on safe dating. Each online safety center must provide:

1. an explanation of the online dating operator's reporting mechanism for harmful or unwanted behavior,

2. safety advice for communicating online and meeting in person,

3. a link to a website or telephone number where a user may access resources on domestic violence and sexual harassment, and

4. educational information on romance scams.

Under the bill, "online dating operators," are defined as anyone who operates a software application designed to facilitate online dating. An "online dating platform" is a digital service designed to allow users to interact through the Internet to initiate relationships with other individuals for romance, sex, or marriage (i.e., "online dating").

Investigations and Penalties for Violations

The bill extends existing penalties and investigatory authority for online dating service notification violations to the bill's online dating

provisions.

In doing so, the bill allows DCP to issue fines of up to $25,000 per violation, accept an offer in compromise, or taking other actions allowed under law or regulations.

It also allows the commissioner or his designee to (1) conduct investigations and hold hearings on any issue related to these provisions and (2) issue subpoenas, administer oaths, compel testimony, and order the production of books, records, and documents.

Under the bill, if anyone refuses to appear, testify, or produce any book, record, or document when ordered to, then the commissioner or his designee may apply to Superior Court for an appropriate enforcement order. Additionally, the bill authorizes the attorney general, at the commissioner's or his designee's request, to apply to Superior Court in the name of the state for an order to restrain and enjoin anyone from violating these provisions.

§ 17 — CT ICAC TASK FORCE

The bill statutorily establishes the CT ICAC within the Department of Emergency Services and Public Protection's Division of Scientific Services and requires it to use appropriated money in a way consistent with specific duties in federal law (i.e., 34 U.S.C. § 21114). This federal law requires each state or local task force that is part of the national program to:

1. consist of state and local investigators, prosecutors, forensic specialists, and education specialists dedicated to addressing the task force goals;

2. work consistently toward achieving ICAC purposes;

3. engage in proactive investigations, forensic examinations, and effective prosecutions of Internet crimes against children;

4. provide forensic, preventive, and investigative assistance to parents, educators, prosecutors, law enforcement, and others

concerned with Internet crimes against children;

5. develop multijurisdictional, multiagency responses and partnerships to investigate and prosecute Internet crimes against children offenses through ongoing informational, administrative, and technological support to other state and local law enforcement agencies, for these agencies to acquire the needed knowledge, personnel, and specialized equipment;

6. participate in nationally coordinated investigations in any case in which the U.S. attorney general determines participation to be needed, as allowed by the task force's available resources;

7. set or adopt investigative and prosecution standards, consistent with established norms, to which the task force must comply;

8. investigate and seek prosecution on tips related to Internet crimes against children, including tips from Operation Fairplay; the National Internet Crimes Against Children Data System; the National Center for Missing and Exploited Children's CyberTipline; ICAC task forces; and other federal, state, and local agencies; with priority given to investigative leads that indicate the possibility of identifying or rescuing child victims, including those that indicate a likelihood of seriousness of offense or danger to the community;

9. develop procedures for handling seized evidence;

10. maintain (a) the required reports and records under the federal law; and (b) other reports and records as the U.S. attorney general determines; and

11. seek to comply with national standards on the investigation and prosecution of Internet crimes against children that the U.S. attorney general sets, to the extent the standards are consistent with Connecticut law.

BACKGROUND

Consumer Data Privacy and Monitoring Law

Beginning July 1, 2023, the consumer data privacy and monitoring law sets a framework for controlling and processing personal data. The framework requires a controller to limit the collection of personal data and establish security practices, among other things. It also gives consumers the right to access, correct, delete, and get a copy of their personal data and to opt out of certain types of personal data processing (e.g., targeted advertising) (CGS § 42-515 et seq.).

Related Bill

sSB 1058 (File 676), § 6, as amended by Senate "A" and passed by the Senate, contains an identical provision prohibiting a controller that has actual knowledge or willfully disregards the consumer's age from processing the consumer's data for targeted advertising without the consumer's consent.

COMMITTEE ACTION

Judiciary Committee

Joint Favorable Substitute
Yea 24 Nay 13 (03/30/2023)