OLR Bill Analysis

sSB 3

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). Among other things, these entities must limit access to consumer health data to individuals and situations specified in the bill. They are also prohibited from collecting or sharing this data without first getting a consumer's consent. The bill also prohibits anyone from selling this data unless a consumer has completed a particular consent form.

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) (§§ 4-6). It specifically requires them to use reasonable care to avoid having their services, products, and features proximately cause, among other things, substantial injury 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 and (2) collecting a minor's precise geolocation data.

Additionally, the bill prohibits certain social media platforms from establishing an account for a minor under age 16 without a parent's or guardian's consent (§ 2). It also requires these platforms to delete a minor's social media account and stop processing the minor's personal data within 10 days after getting a request to delete the account.

Under the bill, any violation of the consumer health data, online services, and social media provisions is deemed a violation under the Connecticut Unfair Trade Practices Act (CUTPA), enforced solely by the attorney general (§§ 1, 2 & 4-6). It further specifies that none of its

provisions may be construed to create a private right of action or grounds for an action under CUTPA.

The bill also:

1. allows courts to order that providers of electronic communication or remote computing services not disclose the existence of a warrant for subscriber or customer records to any person or entity for up to 90 days if a court determines certain exigent or security reasons exist (§ 9);

2. requires online dating operators to owe a duty of care to their users to protect them against potential criminal activity of other users (§§ 10 & 11); and

3. 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 (§ 12).

EFFECTIVE DATE: July 1, 2025, except the CT ICAC provision is effective July 1, 2023, the warrant non-disclosure and online dating operator provisions are effective October 1, 2023, and the social media provision is effective July 1, 2024.

§ 1 — CONSUMER HEALTH DATA DEFINITIONS

The bill sets standards for how regulated entities access and share consumer health data.

Regulated Entity and Consumer

Under the bill, a "regulated entity" is any legal entity that (1) does business in Connecticut or produces or provides goods or services that are targeted to Connecticut consumers and (2) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling consumer health data. It does not include any government agency, tribal nation government organization, or contracted service provider when the provider is processing consumer health data on behalf of a government agency.

The bill defines "consumer" as a state resident but excludes 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 (CGS § 42-515(7)).

Consumer Health Data Generally

For the purposes of the bill, "consumer health data" is any personal information that is linked, or reasonably linkable, to a consumer and identifies the consumer's past, present, or future physical or mental health.

"Personal information" is any information that identifies, or is reasonably capable of being associated or linked, directly or indirectly, with any consumer, including any data associated with a persistent unique identifier such as an Internet browser cookie, Internet protocol address, device identifier, or any other form of persistent unique identifier. It does not include any publicly available information or de-identified data.

"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 a consumer has lawfully made available to the general public (CGS § 42-515(25)). (By law, a "controller" is an individual or legal entity that, 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) (CGS § 42-515(8) & (18)).)

"De-identified data" is data that cannot reasonably be used to infer information about, or otherwise be linked to, a specific individual or his or her device. To be de-identified, a controller that possesses the data must (1) take reasonable measures to ensure the data cannot be associated with the individual, (2) publicly commit to process the data

only in a de-identified fashion and not attempt to re-identify the data, and (3) contractually obligate anyone receiving the data to satisfy these requirements (CGS § 42-515(13)).

Consumer Health Data Inclusions

"Consumer health data" specifically includes any personal information that identifies a consumer's:

1. individual health condition, treatment, status, disease, or diagnosis;
2. social, psychological, behavioral, or medical intervention;
3. health-related surgery or procedure;
4. medication use or purchase;
5. bodily function, vital sign, or symptom (or measurement of any of them);
6. diagnosis or diagnostic testing, treatment, or medication;
7. "gender-affirming care information" (see below);
8. "reproductive or sexual health information" (see below);
9. biometric and genetic data (see below); and
10. "precise location information" (see below) that could reasonably show the consumer's attempt to acquire or receive health services or supplies.

It also includes any information described above that is derived or extrapolated from non-health information such as proxy, derivative, inferred or emergent data derived or extrapolated by any means, including algorithms or machine learning.

Gender-Affirming Care Information and Services. Under the bill, "gender-affirming care information" is any personal information about seeking or getting, past, present, or future gender-affirming care

services, including any of the following:

1. precise location information that could reasonably indicate a consumer's attempt to seek or obtain these services;

2. personal information on any effort made to research or get these services; and

3. information that is derived, extrapolated, or inferred, including from non-health information such as proxy, derivative, inferred, emergent, or algorithmic data.

"Gender-affirming care services" are health services or products that support and affirm any consumer's gender identity, including social, psychological, behavioral, cosmetic, medical, or surgical interventions. They include (1) treatments for gender dysphoria, (2) gender-affirming hormone therapy, and (3) gender-affirming surgical procedures.

Reproductive or Sexual Health Information and Services. For the purposes of the bill, "reproductive or sexual health information" is any personal information about seeking or getting past, present, or future reproductive or sexual health services, including:

1. precise location information that could reasonably show a consumer's attempt to acquire or receive these services;

2. personal information about any effort made to research or obtain these services; and

3. personal information or location information that is derived, extrapolated, or inferred, including from non-health information such as proxy, derivative, inferred, emergent, or algorithmic data.

"Reproductive or sexual health service" is any health service or product that supports or concerns any consumer's reproductive system or sexual well-being, including any that support or concern any:

1. individual health condition, status, disease, or diagnosis;

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

3. health-related surgery or procedure, including an "abortion" (i.e., terminating a pregnancy for any purpose other than producing a live birth);

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

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

6. diagnosis or diagnostic testing, treatment, or medication; and

7. medical or nonmedical service about and provided in conjunction with an abortion, including any diagnostics, counseling, supplies, and follow-up services related to an abortion.

Biometric Data. Under the bill, "biometric data" is data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or identifying characteristics. It does not include digital or physical photographs, video or audio recordings, or data generated from these, unless the data is generated to identify a specific individual (CGS § 42-515(3)).

Genetic Data. For the purposes of the bill, "genetic data" is any data, regardless of format, about a consumer's genetic characteristics including (1) raw sequence data from sequencing all or a portion of a consumer's extracted DNA, (2) genotypic and phenotypic information from analyzing the raw sequence data, and (3) self-reported health data that a consumer submits to a regulated entity and is analyzed in connection with the raw sequence data.

Precise Location Information. Presumably, under the bill, "precise location information" has the same meaning as "precise geolocation data" under existing law, which is information derived from technology, including global positioning system level latitude and

longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. It excludes the content of communications, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility (CGS § 42-515(19)).

Consumer Health Data Exclusions

"Consumer health data" does not include any personal information that is used to engage in any public or peer-reviewed scientific, historical or statistical research if the research (1) is in the public interest, (2) adheres to all other applicable ethics and privacy laws, and (3) is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or another similar independent oversight entity that determines that the regulated entity has implemented reasonable safeguards to mitigate privacy risks associated with the research, including any risks associated with re-identification.

"Process" or "processing" means any manual or automatic operation or set of operations performed on personal data or sets of personal data, including collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data.

§ 1 — CONSUMER HEALTH DATA MANAGEMENT

Access and Security to Consumer Health Data (§ 1(b)(1) & (2))

Regardless of any other state law, the bill requires regulated entities to restrict access to consumer health data by their employees, processors, and contractors to those, presumably, (1) who the consumer has provided consent to access his or her data or (2) where the access is needed to provide a product or service that the consumer has requested from the regulated entity.

Under the bill, "processors" are those who process "personal data" for a "controller" (see above) (CGS § 42-515(21)). Additionally, "consent" is a clear affirmative act signifying the consumer's 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 (CGS § 42-515(6)). 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" (CGS § 42-515(11)).

The bill also requires, regardless of any other state law, each regulated entity must establish, implement, and maintain administrative, technical, and physical data security practices which must at least satisfy a reasonable standard of care within the regulated entity's industry to protect the confidentiality, integrity, and accessibility of consumer health data in an appropriate manner for the volume and nature of the consumer health data.

Prohibition on Collecting and Sharing Consumer Health Data (§ 1(b)(3))

Regardless of any other state law, the bill prohibits regulated entities from collecting or sharing consumer health data about any consumer:

1. without first obtaining his or her consent to do so for a specified purpose;

2. beyond what is reasonably needed, proportionate, and limited to provide or maintain (a) a specific product or service the consumer requested or (b) any communication by the entity to the consumer that is reasonably anticipated within the context of their relationship; or

3. for any purpose that is not expressly allowed under the bill's consumer health data provisions.

Under the bill, "collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any

way.

Additionally, "share" and "sharing" mean any release, disclosure, dissemination, divulsion, making available, access given, licensing, or oral or written communications of consumer health data by a regulated entity to a third party or affiliate. It excludes any disclosure of consumer health data:

1. by a regulated entity to a processor if the disclosure is to provide goods or services in a way that is consistent with the purpose for which the data was collected and disclosed to the consumer; and

2. made to a third party with whom the consumer has a direct relationship when the (a) disclosure is made for the purpose of providing a product or service requested by the consumer, (b) regulated entity maintains control and ownership of the data, and (c) the third party exclusively uses the data at the regulated entity's direction and in a way that is consistent with the purpose for which the data was collected and disclosed to the consumer.

The bill further excludes any disclosure or transfer of consumer health data made to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's assets and complies with the requirements established in the bill's consumer health data provisions.

Under the bill, a "third party" is any entity other than a consumer, regulated entity, or a regulated entity's affiliate. An "affiliate" is any legal entity that (1) shares common branding with another legal entity, and (2) controls, is controlled by, or is under common control with another legal entity through (a) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting securities in either legal entity, (b) control over the election of a majority of the directors of either legal entity or people exercising similar directorial functions of either legal entity, or (c) the power to exercise a controlling influence over the management of either legal entity.

For the purposes of the above prohibition, required consent must, in addition to what is required under its definition, be separately and distinctly obtained for collecting and sharing consumer health data and clearly and conspicuously disclose:

1. the categories of consumer health data collected or shared;

2. the purpose of collecting or sharing the consumer health data, including the specific ways the consumer health data will be used;

3. the categories of entities the consumer health data will be shared with; and

4. how the consumer may withdraw consent from any future collection or sharing of the consumer's consumer health data.

Prohibition on Selling Consumer Health Data (§ 1(c)(1)(A) & (2))

Regardless of any other state law, the bill prohibits anyone from selling, or offering to sell, consumer health data without first getting the consumer's signed, written consent on a specified form. Under the bill, "sale or sell" is sharing consumer health data for monetary or other valuable consideration, except:

1. to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the regulated entity's assets and complies with the requirements in the bill's consumer health data provisions; or

2. by a regulated entity to a processor when sharing the consumer health data is consistent with the purpose for which the consumer health data was collected and disclosed to the consumer.

The form that must be given to consumers before selling or offering to sell their health data must contain:

1. a description of the consumer health data to be offered or sold;

2. the name and contact information for the people who (a) collected and intend to sell, or offer to sell, the consumer health data and (b) intend to buy the data from the collector;

3. a description of the purpose of the proposed offer or sale, including a description of how the consumer health data will be gathered and how the person intending to buy the data plans to use it;

4. statements disclosing that (a) providing the goods or services is not conditioned on the consumer signing the form, (b) the consumer has a right to revoke his or her consent at any time and a description of how he or she may do so, and (c) any consumer health data sold may be subject to redisclosure by a purchasing person and may no longer be protected by the bill following redisclosure;

5. an expiration date for the consent, which may be up to one year after the consumer signs the form; and

6. the consumer's signature and the date the consumer signs the form.

The required form is not valid if:

1. it has expired;

2. it does not satisfy the bill's requirements above;

3. the consumer has revoked his or her consent;

4. it has been combined with any other document for the purpose of getting consent concerning multiple sales, or offers to sell, consumer health data; or

5. the provision of goods or services is conditioned on the consumer signing the form.

The bill requires each person who gives a form to a consumer to also give them a signed copy of it. It also requires each person who sells or

purchases consumer health data to keep a copy of each form for at least six years from when the consumer signed it or the last date it was effective, whichever is later.

Prohibition on Using Geofences (§ 1(c)(1)(B))

Regardless of any other state law, the bill prohibits anyone from implementing a geofence to identify, track, collect data from or send notifications or messages to a consumer that enters the virtual perimeter around a health care provider or health care facility providing health care services on an in-person basis.

Under the bill, a "geofence" is any technology that uses global positioning coordinates, 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 that is within 2,000 feet of the perimeter around any physical location. A "health care service" is generally any service provided to any consumer to assess, measure, improve, or learn about the consumer's health.

Restrictions on Processing Consumer Health Data (§ 1(d))

The bill allows a processor to process consumer health data only by a binding contract between the processor and a regulated entity. The contract must provide the processing instructions for and limit the actions which the processor may take with respect to the consumer health data the processor processes on the regulated entity's behalf.

The bill prohibits processors from processing consumer health data in way that is inconsistent with the contract terms. The processor must assist the regulated entity by taking all appropriate and possible technical and organizational measures needed for the regulated entity to do the entity's duties under the bill's consumer health data provisions. If the processor fails to adhere to the regulated entity's processing instructions or processes consumer health data in a manner outside the scope of the contract, the processor is deemed to constitute a regulated entity and is subject to the bill's regulated entity requirements.

Under the bill, "process" and "processing" mean any operation or set of operations done on consumer health data.

§§ 3-6 & 8 — 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., those under age 18 who are consumers). Under the bill, "online service, product, or feature" is any service, product, or feature that is provided online, but excludes any (1) telecommunications service, or (2) delivery or use of a physical product. "Controllers," "process," "consent," "personal data," and "consumers" have the same meanings as above (see § 1).

Avoiding Heightened Risk of Harm to Minors (§ 4(a))

If a controller offers an online service, product, or feature to consumers who 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 proximately cause any heightened risk of harm to minors.

Under the bill, "heightened risk of harm to minors" is processing minors' personal data, including through using any "algorithm" (i.e., any computerized procedure with a set of steps used to accomplish a predetermined objective), 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;

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; or

4. other substantial injury to minors.

Collecting Minors' Precise Geolocation Data and Processing Minors' Personal Data (§ 4(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 prohibits the controller from collecting minors' precise geolocation data and processing their personal data 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.

The bill also prohibits these controllers from collecting a minor's "precise geolocation data" (see definition in § 1 above) unless (1) the data is 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 conspicuous to the minor for the entire time.

The bill also 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 decision the controller makes resulting in the controller providing or denying any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services;

2. that is not reasonably necessary to provide the online service, product, or feature;

3. for any processing purpose other than the disclosed purpose at the time the controller collected the personal data;

4. for longer than is reasonably necessary to provide the online

service, product, or feature; or

5. in any circumstances in which the minor's personal data is accessible by, or visible to, any other user of the online service, product, or feature.

Under the bill, "targeted advertising" is displaying an advertisement to a minor based on profiling. It does not include an advertisement that is (1) based on the context of a minor's current search query, visit to a website, or online application, or (2) directed to a minor in response to his or her current request for information or feedback. It also excludes processing personal data solely to measure or report 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 (§ 4(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. using any user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, including any practice the Federal Trade Commission refers to as a "dark pattern," to lead or encourage any minor to provide any personal data that is not reasonably necessary to provide the online service, product, or feature;

2. by default, using any system design feature to increase, sustain, or extend any minor's use of the online service, product, or feature by, among other things, automatically playing any media, offering any reward to encourage the minor to spend time using the online service, product, or feature, or sending notifications to the minor;

3. allowing any minor's parent, legal guardian, or any other consumer to monitor the minor's online activity unless the controller provides the minor a signal, which is obvious to the minor, that he or she is being monitored; or

4. allow any adult to contact any minor through any messaging apparatus unless the adult previously established and maintains an ongoing, lawful relationship with the minor.

Data Protection Assessment (§ 5)

The bill requires each controller that, on or after July 1, 2025, 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 in the data protection

assessment required under the state's consumer data privacy and online monitoring law (CGS § 42-522, see BACKGROUND). (It is not clear which specific requirements apply to the bill's assessment.)

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 at least biennially and (2) maintain documentation on the assessment as long as the controller offers the online service, product, or feature to minors. 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 before offering the service, product, or feature to consumers who they have actual knowledge, or willfully disregard, are minors.

Processors' Duties and Contracts With Controllers (§ 6)

The bill imposes the same obligations to controllers' processors as under the state's existing consumer data privacy and online monitoring law (CGS § 42-521). This includes adhering to the controller's instructions and helping them meet their obligations under the bill and providing the needed information for controllers to do data protection assessments.

Contract. Under the bill, a contract between a processor and controller must 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.

Violations (§ 8)

From July 1, 2025, to December 31, 2027, 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, 2027, the attorney general must submit a report to the General Law Committee disclosing:

1. the number of notices of violations he issued,
2. the nature of each violation,
3. the number of violations cured within the 30-day period, and

4. any other matters he deems relevant.

Beginning on January 1, 2027, 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, and
5. whether the alleged violation was likely caused by human or technical error.

§ 7 — EXEMPTIONS AND CONSTRUCTION OF CONTROLLERS' AND PROCESSORS' DUTIES

Exemptions

As under the state's existing consumer data privacy and online monitoring law (CGS § 42-517), the bill's provisions on consumer health data and online services do not apply to certain entities. This includes the following:

1. state bodies, authorities, boards, bureaus, commissions, districts, or agencies or those of its political subdivisions;
2. federally tax-exempt nonprofit organizations;
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.); or
5. covered entities or business associates, as defined in HIPAA regulations (e.g., health plans, health care clearinghouses, and health care providers).

The bill also exempts:

1. entities licensed or accredited to offer one or more programs of higher learning that lead to at least one degree; and

2. any air carrier (i.e., a U.S. citizen that provides air transportation by any means) that is 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).

As under the consumer data privacy and online monitoring law, the bill also exempts certain information and data. Specifically, 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, 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 in the federal Airline Deregulation Act (49 U.S.C. § 40101 et seq.), by an air carrier subject to that bill, to the extent this bill is preempted by the Airline Deregulation Act (49 U.S.C. § 41713).

Ability to Collect, Use, or Retain Data

As under the consumer data privacy and online monitoring law (CGS § 42-524), the bill also specifies that the bill's obligations on consumer health data and online services that it imposes on controllers and processors do not restrict their ability to collect, use, or retain data for internal use to:

1. do 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 minor's expectations, reasonably anticipated based on the minor's existing relationship with the controller, or compatible with processing data based on providing a product or service the minor specifically requested.

Evidentiary Privilege

The bill's obligations on consumer health data and online services

that it imposes on controllers or processors do not apply if doing so would make them violate state evidentiary privilege. The bill should not be construed to prevent a controller or processor from giving personal data about a minor to a person covered by state evidentiary privilege laws as a privileged communication.

First Amendment Rights

The bill states that its provisions on consumer health data and online services are not to 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). It also does not affect a person processing personal data for a purely personal or household activity.

Limitations on Processing Personal Data

Under the bill, controllers may process personal data to the extent the processing is (1) reasonably necessary and proportionate to the purposes listed above (e.g., for internal research) 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 minors related to its collection, use, or retention.

Under the bill, if a controller or processor processes personal data for a specified purpose through one of the exemptions listed above, the respective controller or processor bears the burden of showing that the processing (1) qualifies for an exemption under the bill and (2) complies with the bill's requirements for processing personal data.

§ 2 — SOCIAL MEDIA PLATFORMS AND MINORS

The bill prohibits social media platforms from establishing an account for a minor under age 16 without a parent's or guardian's

consent.

It also requires these platforms to delete a minor's account within 10 days of getting a request from (1) the minor if he or she is age 16 or older but younger than age 18 or (2) the minor's parent or legal guardian if the minor is under age 16. The platform must also, within this timeframe, stop processing the minor's "personal data" (see definition in § 1 above). Relatedly, the bill requires platforms to establish and describe in a privacy notice one or more secure and reliable way of submitting an account deletion request.

Under the bill a "social media platform" is a public or semi-public Internet-based service or application that:

1. is used by a "consumer" (see definition in § 1 above) in Connecticut;

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

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

"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; or

2. primarily consists of news, sports, entertainment, 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.

§ 9 — WARRANT

The bill allows courts to order providers of electronic communications or remote computing services not to disclose the existence of a warrant for a subscriber or customer record to any other person or entity for up to 90 days for certain exigent or security reasons. A court may make this order if it believes the notification will result in:

1. endangering the life or physical safety of an individual;
2. flight from prosecution;
3. destruction of or tampering with evidence;
4. intimidation of potential witnesses; or
5. otherwise seriously jeopardizing the investigation.

Under the bill, an "electronic communication service" is any service that enables its users to send or receive wire or electronic communications. A "remote computing service" involves providing computer storage or processing services to the public by means of an electronic communications system (CGS § 54-47aa and 18 U.S.C. §§ 2510 & 2711).

§§ 10 & 11 — ONLINE DATING OPERATORS

Under the bill, an online dating operator owes a duty of care to any online dating platform user to protect him or her against potential criminal activity of other users. This includes a duty to notify users if the online dating operator has had a communication with another user that the operator determines to have a higher propensity to commit a crime against individuals. (It is unclear what is considered having a higher propensity to commit a crime against individuals or how an operator would make this determination.)

Under the bill, "online dating operators," are defined as anyone who operates a software application (e.g., presumably, an online dating platform) 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").

§ 12 — 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.).

COMMITTEE ACTION

Judiciary Committee

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