PA 23-56—sSB 3
Judiciary Committee

AN ACT CONCERNING ONLINE PRIVACY, DATA AND SAFETY PROTECTIONS

SUMMARY: This act makes various changes to laws on data privacy and related issues, including provisions on consumer health data, minors' social media accounts and online services, online dating operators, and a task force on Internet crimes against children.

The act sets standards on accessing and sharing consumer health data (§§ 1 & 2). For example, the act generally prohibits individuals or business entities 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 on consumer data privacy and online monitoring and makes other changes to the existing data privacy law (§§ 1 & 3-6).

The act's provisions on consumer health data and consumer health data controllers generally apply to individuals or entities that conduct business in Connecticut or produce products or services 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 gross revenue from selling personal data.

The act requires social media platforms to unpublish a minor's social media account within 15 business days, and generally delete the account within 45 business days, after receiving an authenticated request (§ 7).

It 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. It also prohibits them 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 the online service, product, or feature; and (3) collecting a minor's precise geolocation data.

Under the act, any violation of its consumer health data, social media, or online services provisions is a Connecticut Unfair Trade Practices Act (CUTPA) violation, enforced solely by the attorney general (§§ 6, 7 & 13). The act 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. (PA 23-204, §§ 208 & 450, repeals and replaces

the provisions on enforcement of the consumer health data provisions to align with that act's delayed effective date for these provisions.)

The act 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 (CT ICAC) task force and requires it to use appropriated state and federal funding in a way that is consistent with its duties under federal law (§ 17).

EFFECTIVE DATE: July 1, 2023, except the online dating provisions are effective January 1, 2024, the social media provisions are effective July 1, 2024, and the minors and online services provisions are effective October 1, 2024 (PA 23-204, § 207, delays the effective date until October 1, 2023, for the provisions on consumer health data and changes to the existing data privacy and online monitoring law).

§ 1 — CONSUMER HEALTH DATA DEFINITIONS

Consumer Health Data Generally

For purposes of the act, "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 (see below).

As under the state's 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 an individual or legal entity (e.g., associations and corporations) 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 act, 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 act, "gender-affirming health data" is any personal data about a consumer's efforts to seek, or receiving of, gender-affirming health care services. "Gender-affirming health care services" is all medical care related to the treatment of gender dysphoria. (PA 23-204 expands this definition; see BACKGROUND, *Related Acts.*)

Reproductive or Sexual Health Data

Under the act, "reproductive or sexual health data" is any personal data about a consumer's effort to seek, or a consumer's receipt of, reproductive or sexual health care.

"Reproductive or sexual health care" is any health care-related 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 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 act prohibits specific actions relating to consumer health data, as follows.

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

The act generally prohibits anyone from giving any employee or contractor 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 giving a processor 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 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 act 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 act, 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 act 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 using dark patterns. A "dark pattern" is a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, and includes any practice the Federal Trade Commission refers to as a "dark pattern."

§§ 2 & 3 — EXEMPTIONS FROM DATA PRIVACY LAWS

The act'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 act'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, including health plans, health care clearinghouses, and health care providers.

The act also exempts the following individuals and entities 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 as defined and regulated under federal law.

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

The state's existing consumer data privacy and online monitoring law also exempts from its requirements specified information and data (e.g., protected health information under HIPAA, identifiable private information for human research, certain credit-related information, and certain information collected under specified federal laws; see CGS § 42-517(b) as amended by this act). The act exempts the same information and data from its consumer health data provisions. It also adds to the list of exemptions from the existing consumer data privacy law (and the act's consumer health data provisions) data that is processed or maintained while an individual is applying to, employed by, or contracting with a consumer health data controller.

Parental Consent Exemption (§ 3(c))

Under the existing consumer data privacy and online monitoring law, 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.) are deemed compliant with any obligation to obtain parental consent under the law.

The act extends this exemption to consumer health data controllers that comply with COPPA's verifiable parental consent requirements.

§ 5 — PROCESSING PERSONAL DATA FOR SPECIFIED PURPOSES

The act specifically extends several existing provisions of the consumer data privacy and online monitoring law to apply to consumer health data controllers. For example, it specifies the following:

1. Nothing under the act's health data requirements (see § 2 above) or existing law should be construed to restrict a consumer health data controller's ability to comply with certain requirements or take specified other actions, such as cooperating with law enforcement under specified conditions or providing a product or service that a consumer specifically requested (§ 5(a)); see CGS § 42-524, as amended by this act).
2. The obligations that existing law and the act impose on consumer health data controllers do not restrict their ability to collect, use, or retain data for internal use for specified purposes (§ 5(b)).
3. Consumer health data controllers that disclose personal data to a processor or third-party controller under the act's or existing law's requirements are

not responsible for violations by them if, at the time of disclosure, the original consumer health data controller did not have actual knowledge that the recipient would violate the act or law (§ 5(d)).

4. If a consumer health data controller processes personal data for a specified purpose through one of the specified exemptions, then that controller bears the burden of showing that the processing qualifies for an exemption and complies with the requirements for processing personal data (§ 5(g)).

§ 6 — ATTORNEY GENERAL'S POWERS

The act extends existing law's enforcement provisions to its new provisions on consumer health data controllers as follows:

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 a violation if he determines that a cure is possible.
3. Starting January 1, 2025, the attorney general has discretion over whether to provide an opportunity to correct an alleged violation.
4. The act's provisions should not be construed as providing the basis for, or be subject to, a private right of action for violations under the act or any other law.
5. Any violation of the act'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.

(PA 23-204, §§ 208 & 450, repeals and replaces these enforcement provisions to align with that act's delayed effective date for the consumer health data privacy provisions.)

Notice of and Opportunity to Correct Violations

From July 1, 2023, to December 31, 2024, the act, as under existing law, requires the attorney general to issue a violation notice to a consumer health data controller if he determines a cure is possible before initiating any action for a violation of its provisions. If the controller fails to cure the violation within 60 days after receiving notice, the attorney general may bring an action. (PA 23-204, §§ 208 & 450, delays the start of this period from July 1, 2023, to October 1, 2023, for consumer health data controllers to align with that act's delayed effective date for these provisions.)

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

Violations On or After January 1, 2025

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

violation:

1. the number of violations,
2. the controller's size and complexity and the nature and extent of its processing activities,
3. the substantial likelihood of injury to the public,
4. the safety of people or property, and
5. whether the alleged violation was likely caused by human or technical error.

The act additionally allows him to consider the sensitivity of the data for alleged violations by consumer health data controllers and other controllers or processors.

§§ 1 & 4 — 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 a consumer without consent, or if the consumer is a known child (i.e., younger than age 13), if the data is not processed in accordance with COPPA (see § 4(a)(4)). Controllers must also conduct and document a data protection assessment for each of their processing activities that presents a heightened risk of harm to consumers, including the processing of sensitive data (CGS § 42-522(a)).

The act expands the definition of "sensitive data" for these purposes to cover personal data that includes consumer health data or 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).

Prohibition on Certain Actions as to Minors (§ 4)

Existing law prohibits controllers from processing a consumer's personal data for targeted advertising, or selling the data without the consumer's consent, for consumers ages 13-15. Under prior law, for the prohibition to apply, the controller had to have actual knowledge that the consumer's age was in this range and willfully disregard it. Under the act, 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 act 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 the minor's account (i.e., remove it from public visibility) within 15 business days after receiving the request.

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

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

A social media platform is not 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 act also requires a social media platform to delete the minor's social media platform account within 45 business days after receiving the request. The platform must delete the account and stop processing the minor's personal data except where preserving the account or data is otherwise permitted or required by law. A platform may extend this period by another 45 business days if the extension is reasonably necessary when considering the complexity and number of consumer requests. The platform must inform the person making the request within the initial 45 business days about the extension and reason for it.

Privacy Notice

The act requires a social media platform to establish and describe in a privacy notice, at least one secure and reliable way to submit a request to unpublish and delete an account. A platform that provides a mechanism to initiate this process is deemed in compliance with the unpublish and deletion requirements.

Inability to Authenticate

Under the act, a platform does not have to comply with a request that it cannot authenticate. But it must notify the consumer who submitted the request that it cannot authenticate the request and will not be able to do so until the consumer provides additional reasonably necessary information. Under the act, to "authenticate" is using reasonable means and making a commercially reasonable

effort to determine whether a request to unpublish and delete data was made by or on behalf of the minor with the right to make the request.

Violations

Under the act, a violation of the social media account provisions is a CUTPA violation that 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 act also establishes a framework and sets requirements for how controllers who offer online services, products, and features manage, process, and get consent to use the personal data of minors (i.e., consumers under age 18). Under the act, an "online service, product, or feature" is any service, product, or feature provided online, but not 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 above).

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

The act requires a controller with minor customers to use reasonable care to avoid causing any heightened risk of harm to minors. This applies if the controller offers an online service, product, or feature to consumers for whom it has actual knowledge, or willfully disregards knowing, are minors.

Under the act, "heightened risk of harm to minors" is processing minors' personal data, including in a way that presents any reasonably foreseeable risk of any of the following:

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.

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

The act generally prohibits a controller with minor customers (see above) from taking certain actions 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. These actions include (1) collecting the minor's 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. A controller can satisfy this requirement by complying with the verifiable parental consent requirements of the federal COPPA.

Geolocation. Specifically, the act prohibits these controllers from collecting a minor's precise geolocation data unless the (1) 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) 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.

Personal Data. The act specifically prohibits these controllers from processing any minor's personal data:

1. for (a) targeted advertising, (b) personal data sales, 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; or
4. for longer than is reasonably necessary to provide the online service, product, or feature.

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

Under the act, "targeted advertising" is 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(30), as amended by this act).

"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) when 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(37), as amended by this act).

Interface Prohibitions (§ 9(c))

The act also prohibits a controller with minor customers from:

1. providing any consent mechanism designed to substantially subvert or impair, or 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 act requires each controller with minor customers, on or after October 1, 2024, to do a data protection assessment of its online service, product, or feature. The assessment must be done consistently with the applicable requirements under the state's consumer data privacy and online monitoring law (CGS § 42-522).

The act requires the assessment to 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 for 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 act, each controller that does a data protection assessment must (1) review the assessment as needed to account for any material change to the processing operations of the online service, product, or feature that is the subject of the assessment and (2) maintain documentation on the assessment for the longer of

(a) the three-year period beginning when the processing operation ends or (b) as long as the controller offers the online service, product, or feature.

The act 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 satisfies the act's assessment requirement if it is reasonably similar in scope and effect.

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

Under the act, 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 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 act requires processors to adhere to the controller's instructions and help them meet their obligations under the act's online services provisions, considering (1) the nature of the processing, (2) the information available to the processor by appropriate technical and organizational measures, and (3) whether the assistance is reasonably practicable and needed to help the controller meet its obligations. Processors must also provide the needed information for controllers to do data protection assessments.

Contract. The act applies the same contract requirements that apply under the consumer data privacy and online monitoring law to processors and controllers subject to the act's provisions on minors and online services. Thus, the act 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 needed to show the processor's compliance with the obligations under the data privacy and online monitoring law;
4. after giving the controller an opportunity to object, engage any subcontractor under 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.

As under the data privacy and online monitoring law, the act requires an independent assessor to evaluate the processor's policies and technical and organizational measures regarding the act'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. These requirements must 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 or Processor. Under the act, 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 for 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 act'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 act exempts from the above requirements certain entities, information, and data (see CGS § 42-517, as amended by the act, and see § 3 above, except the act's provisions on minors and online services do not exempt those who contract with state and local governmental entities or certain consumer health-related data).

Ability to Comply With Certain Requirements or Take Specified Other Actions. Substantially similar to the consumer data privacy and online monitoring law, the act'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 act, and § 5(a) above, except for certain provisions related to consumer-selected services or consumer contracts; see § 5(a)(5)-(7)).

As under the consumer data privacy and online monitoring law, as amended by the act, the act also specifies that the obligations it imposes on controllers and processors do not:

1. restrict their ability to collect, use, or retain data for internal use (see § 5(b)) and
2. apply if doing so would make them violate state evidentiary privilege (see § 5(c)).

The act also specifies that the obligations it imposes on controllers do not adversely affect 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 (see § 5(e)).

Finally, as under the consumer data privacy and online monitoring law, the act limits controllers' processing of personal data (e.g., it must be limited to what is

needed for the specific listed purpose) and places the burden on the controller to show that the processing qualifies for an exemption and is compliant (see § 5(f) & (g)).

Violations (§§ 9 & 13)

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

Within 30 days after getting this notice, the controller or processor may send notice to the attorney general, on a form he prescribes, stating 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 act, 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, in determining whether to give a controller or processor the opportunity to cure an alleged violation, the attorney general may 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.

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

§§ 14-16 — ONLINE DATING OPERATORS

Required Policies and Online Safety Center

The act 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 act, an "online dating operator" is 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 act extends existing penalties and investigatory authority for online dating service notification violations to the act's online dating provisions.

In doing so, the act allows the Department of Consumer Protection to issue fines of up to $25,000 per violation, accept an offer in compromise, or take 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 act, 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 act 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 act statutorily establishes the Connecticut Internet Crimes Against Children (CT ICAC) task force within the Department of Emergency Services and Public Protection's (DESPP) 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).

The 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 necessary 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 they are consistent with Connecticut law.

(Among other things, PA 23-204, §§ 326 & 327, for FYs 25 and 26, requires DESPP to establish an investigative unit within the CT ICAC task force to conduct sting operations relating to the online sexual abuse of minors.)

BACKGROUND

Consumer Data Privacy and Online Monitoring Law

Beginning July 1, 2023, the consumer data privacy and online monitoring law sets a framework for controlling and processing personal data. The framework requires a controller to limit personal data collection 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 Acts

PA 23-98, § 6, 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.

PA 23-204, § 307, (1) expands the definition of "gender-affirming health care

services" used in this act to include gender incongruence and (2) specifies that, for purposes of this definition, gender dysphoria is based on the most recent edition of the American Psychiatric Association's "Diagnostic and Statistical Manual of Mental Disorders."