Senate

General Assembly

File No. 576

January Session, 2025

Substitute Senate Bill No. 1295

Senate, April 8, 2025

The Committee on General Law reported through SEN. MARONEY of the 14th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

AN ACT CONCERNING SOCIAL MEDIA PLATFORMS AND ONLINE SERVICES, PRODUCTS AND FEATURES.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective October 1, 2025*) (a) As used in this section:

(1) "Consumer" means an individual who is a resident of this state and a user of a social media platform;

(2) "Cyberbullying" means any unwanted and aggressive behavior on a social media platform;

(3) "Mental health services" has the same meaning as provided in section 19a-498c of the general statutes;

(4) "Owner" means the person who owns a social media platform;

(5) "Person" means an individual, association, corporation, limited liability company, partnership, trust or other legal entity; and

(6) "Social media platform" has the same meaning as provided in section 42-528 of the general statutes.

(b) Not later than January 1, 2026, each owner of a social media platform shall incorporate an online safety center into the social media platform. Each online safety center shall, at a minimum, provide the consumers who use such social media platform with:

(1) Resources for the purposes of (A) preventing cyberbullying on such social media platform, and (B) enabling any consumer to identify any means available to such consumer to obtain mental health services, including, but not limited to, an Internet web site address or telephone number where such consumer may obtain mental health services for the treatment of an anxiety disorder or the prevention of suicide;

(2) Access to online behavioral health educational resources;

(3) An explanation of such social media platform's mechanism for reporting harmful or unwanted behavior, including, but not limited to, cyberbullying, on such social media platform; and

(4) Educational information concerning the impact that social media platforms have on users' mental health.

(c) Not later than January 1, 2026, each owner of a social media platform shall establish a cyberbullying policy for the social media platform. Such policy shall, at a minimum, set forth the manner in which such owner handles reports of cyberbullying on such social media platform.

Sec. 2. Section 42-529 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

For the purposes of this section and sections 42-529a to 42-529e, inclusive, as amended by this act:

(1) "Adult" means any individual who is at least eighteen years of age;

(2) "Consent" has the same meaning as provided in section 42-515;

(3) "Consumer" has the same meaning as provided in section 42-515;

(4) "Controller" has the same meaning as provided in section 42-515;

(5) "Heightened risk of harm to minors" means processing minors' personal data in a manner that presents any reasonably foreseeable risk of (A) any unfair or deceptive treatment of, or any unlawful disparate impact on, minors, (B) any financial, physical or reputational injury to minors, **[**or**]** (C) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person, (D) any anxiety or depressive disorder in minors, which disorder has objectively verifiable and clinically diagnosable symptoms and is related to compulsive use of any online service, product or feature by minors, (E) any compulsive use of any online service, product or feature by minors, (F) any physical violence against minors, (G) any harassment of minors on any online service, product or feature, which harassment is so severe, pervasive or objectively offensive as to impact one or more major life activities of minors, (H) any sexual abuse or sexual exploitation of minors, (I) any unlawful distribution or sale to minors of, or any consumption or use by minors of, any alcoholic beverage, as defined in section 30-1, cannabis, as defined in section 21a-420, cigarette, as defined in section 12-285, electronic nicotine delivery system, as defined in section 21a-415, infused beverage, as defined in section 21a-425, moderate-THC hemp product, as defined in section 21a-426, narcotic substance, as defined in section 21a-240, tobacco product, as defined in section 12-330a, or vapor product, as defined in section 21a-415, or (J) any unlawful gambling by minors;

(6) "HIPAA" has the same meaning as provided in section 42-515;

(7) "Minor" means any consumer who is younger than eighteen years of age;

(8) "Online service, product or feature" means any service, product or feature that is provided online. "Online service, product or feature" does not include any (A) telecommunications service, as defined in 47 USC

153, as amended from time to time, (B) broadband Internet access service, as defined in 47 CFR 54.400, as amended from time to time, or (C) delivery or use of a physical product;

(9) "Person" has the same meaning as provided in section 42-515;

(10) "Personal data" has the same meaning as provided in section 42-515;

(11) "Precise geolocation data" has the same meaning as provided in section 42-515;

(12) "Process" and "processing" have the same meaning as provided in section 42-515;

(13) "Processor" has the same meaning as provided in section 42-515;

(14) "Profiling" has the same meaning as provided in section 42-515;

(15) "Protected health information" has the same meaning as provided in section 42-515;

(16) "Sale of personal data" has the same meaning as provided in section 42-515;

(17) "Targeted advertising" has the same meaning as provided in section 42-515; and

(18) "Third party" has the same meaning as provided in section 42-515.

Sec. 3. Section 42-529a of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(a) Each controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or **[**wilfully disregards**]** knowledge fairly implied based on objective circumstances, are minors shall use reasonable care to avoid any heightened risk of harm to minors caused by such online service, product or feature. In any

enforcement action brought by the Attorney General pursuant to section 42-529e, there shall be a rebuttable presumption that a controller used reasonable care as required under this section if the controller complied with the provisions of section 42-529b, as amended by this act, concerning data protection assessments and impact assessments.

(b) (1) [Subject to the consent requirement established in subdivision (3) of this subsection, no] No controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or [wilfully disregards] knowledge fairly implied based on objective circumstances, are minors shall [: (A) Process] process any minor's personal data: [(i) for] (A) For the purposes of [(I)] (i) targeted advertising, [(II)] (ii) any sale of personal data, or [(III)] (iii) profiling in furtherance of any [fully] automated decision made by such controller that produces any legal or similarly significant effect concerning the provision or denial by such controller of 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; [, (ii)] (B) unless such processing is reasonably necessary to provide such online service, product or feature; [, (iii)] (C) for any processing purpose [(I)] (i) other than the processing purpose that the controller disclosed at the time such controller collected such personal data, or [(II)] (ii) that is reasonably necessary for, and compatible with, the processing purpose described in subparagraph [(A)(iii)(I)] (C)(i) of this subdivision; [,] or [(iv)] (D) for longer than is reasonably necessary to provide such online service, product or feature. [; or (B) use any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature.] The provisions of this subdivision shall not apply to any service or application that is used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program.

(2) [Subject to the consent requirement established in subdivision (3) of this subsection, no] No controller that offers an online service, product or feature to consumers whom such controller has actual

knowledge, or [wilfully disregards] knowledge fairly implied based on objective circumstances, are minors shall collect a minor's precise geolocation data unless: (A) Such precise geolocation data is reasonably necessary for the controller to provide such online service, product or feature and, if such data is necessary to provide such online service, product or feature, such controller may only collect such data for the time necessary to provide such online service, product or feature; and (B) the controller provides to the minor a signal indicating that such controller is collecting such precise geolocation data, which signal shall be available to such minor for the entire duration of such collection.

[(3) No controller shall engage in the activities described in subdivisions (1) and (2) of this subsection unless the controller obtains the minor's consent or, if the minor is younger than thirteen years of age, the consent of such minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time, shall be deemed to have satisfied any requirement to obtain parental consent under this subdivision.]

(c) (1) No controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or [wilfully disregards] knowledge fairly implied based on objective circumstances, are minors shall: (A) Provide any consent mechanism that is designed to substantially subvert or impair, or is manipulated with the effect of substantially subverting or impairing, user autonomy, decision-making or choice; [or] (B) except as provided in subdivision (2) of this subsection, offer any direct messaging apparatus for use by minors [without providing] unless (i) such controller provides readily accessible and easy-to-use safeguards to [limit the ability of adults to send] enable any minor, or any minor's parent or legal guardian, to prevent any adult from sending any unsolicited [communications to minors with whom they are not connected] communication to such

minor unless such minor and adult are already connected on such online service, product or feature, and (ii) the safeguards required under subparagraph (B)(i) of this subdivision, as a default setting, prevent any adult from sending any unsolicited communication to any minor unless such minor and adult are already connected on such online service, product or feature; or (C) except as provided in subdivision (3) of this subsection, use any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature.

(2) The provisions of subparagraph (B) of subdivision (1) of this subsection shall not apply to services where the predominant or exclusive function is: (A) Electronic mail; or (B) direct messaging consisting of text, photos or videos that are sent between devices by electronic means, where messages are (i) shared between the sender and the recipient, (ii) only visible to the sender and the recipient, and (iii) not posted publicly.

(3) The provisions of subparagraph (C) of subdivision (1) of this subsection shall not apply to any service or application that is used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program.

Sec. 4. Section 42-529b of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(a) Each controller that **[**, on or after October 1, 2024,**]** offers any online service, product or feature to consumers whom such controller has actual knowledge, or **[**wilfully disregards**]** knowledge fairly implied based on objective circumstances, are minors shall conduct a data protection assessment for such online service, product or feature: (1) In a manner that is consistent with the requirements established in section 42-522; and (2) that addresses (A) the purpose of such online service, product or feature, (B) the categories of minors' personal data that such online service, product or feature processes, (C) the purposes for which such controller processes minors' personal data with respect to such

online service, product or feature, and (D) any heightened risk of harm to minors that is a reasonably foreseeable result of offering such online service, product or feature to minors.

(b) Each controller that offers any online service, product or feature to consumers whom such controller has actual knowledge, or knowledge fairly implied based on objective circumstances, are minors shall, if such online service, product or feature engages in any profiling based on such consumers' personal data, conduct an impact assessment for such online service, product or feature. Such impact assessment shall include, to the extent reasonably known by or available to the controller, as applicable: (1) A statement by the controller disclosing the purpose, intended use cases and deployment context of, and benefits afforded by, such online service, product or feature, if such online service, product or feature engages in any profiling for the purpose of making decisions that produce legal or similarly significant effects concerning such consumers; (2) an analysis of whether such profiling poses any known or reasonably foreseeable heightened risk of harm to minors and, if so, (A) the nature of such heightened risk of harm to minors, and (B) the steps that have been taken to mitigate such heightened risk of harm to minors; (3) a description of (A) the categories of personal data such online service, product or feature processes as inputs for the purposes of such profiling, and (B) the outputs such online service, product or feature produces for the purposes of such profiling; (4) an overview of the categories of personal data the controller used to customize such online service, product or feature for the purposes of such profiling, if the controller used data to customize such online service, product or feature for the purposes of such profiling; (5) any metrics used to evaluate the performance and known limitations of such online service, product or feature for the purposes of such profiling; (6) a description of any transparency measures taken concerning such online service, product or feature with respect to such profiling, including, but not limited to, any measures taken to disclose to consumers that such online service, product or feature is being used for such profiling while such online service, product or feature is being used for such profiling; and (7) a description of the post-deployment monitoring and user

safeguards provided concerning such online service, product or feature for the purposes of such profiling, including, but not limited to, the oversight, use and learning processes established by the controller to address issues arising from deployment of such online service, product or feature for the purposes of such profiling.

[(b)**]** (c) Each controller that conducts a data protection assessment pursuant to subsection (a) of this section, or an impact assessment pursuant to subsection (b) of this section, shall: (1) Review such data protection assessment or impact assessment as necessary to account for any material change to the processing or profiling operations of the online service, product or feature that is the subject of such data protection assessment or impact assessment; and (2) maintain documentation concerning such data protection assessment or impact assessment for the longer of (A) the three-year period beginning on the date on which such processing or profiling operations cease, or (B) as long as such controller offers such online service, product or feature.

[(c)**]** (d) A single data protection assessment or impact assessment may address a comparable set of processing or profiling operations that include similar activities.

[(d)**]** (e) If a controller conducts a data protection assessment or impact assessment for the purpose of complying with another applicable law or regulation, the data protection assessment or impact assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment or impact assessment is reasonably similar in scope and effect to the data protection assessment or impact assessment that would otherwise be conducted pursuant to this section.

[(e)**]** (f) If any controller conducts a data protection assessment pursuant to subsection (a) of this section, or an impact assessment pursuant to subsection (b) of this section, and determines that the online service, product or feature that is the subject of such assessment poses a heightened risk of harm to minors, such controller shall establish and implement a plan to mitigate or eliminate such risk. The Attorney

General may require a controller to disclose to the Attorney General a plan established and implemented pursuant to this subsection if the plan is relevant to an investigation conducted by the Attorney General.

[(f)**]** (g) Data protection assessments and impact assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200. To the extent any information contained in a data protection assessment or impact assessment disclosed to the Attorney General includes information subject to the attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

Sec. 5. Section 42-529c of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2025*):

(a) A processor shall adhere to the instructions of a controller, and shall: (1) Assist the controller in meeting the controller's obligations under sections 42-529 to 42-529e, inclusive, as amended by this act, taking into account (A) the nature of the processing, (B) the information available to the processor by appropriate technical and organizational measures, and (C) whether such assistance is reasonably practicable and necessary to assist the controller in meeting such obligations; and (2) provide any information that is necessary to enable the controller to conduct and document data protection assessments and impact assessments pursuant to section 42-529b, as amended by this act.

(b) Each processor that offers any online service, product or feature to consumers whom such processor has actual knowledge, or knowledge fairly implied based on objective circumstances, are minors shall, if such online service, product or feature engages in any profiling based on such consumers' personal data, conduct an impact assessment for such online service, product or feature. Such impact assessment shall include, to the extent reasonably known by or available to the processor, as applicable: (1) A statement by the processor disclosing the purpose, intended use cases and deployment context of, and benefits afforded by, such online service, product or feature, if such online service, product or feature engages in any profiling for the purpose of making decisions

that produce legal or similarly significant effects concerning such consumers; (2) an analysis of whether such profiling poses any known or reasonably foreseeable heightened risk of harm to minors and, if so, (A) the nature of such heightened risk of harm to minors, and (B) the steps that have been taken to mitigate such heightened risk of harm to minors; (3) a description of (A) the categories of personal data such online service, product or feature processes as inputs for the purposes of such profiling, and (B) the outputs such online service, product or feature produces for the purposes of such profiling; (4) an overview of the categories of personal data the processor used to customize such online service, product or feature for the purposes of such profiling, if the processor used data to customize such online service, product or feature for the purposes of such profiling; (5) any metrics used to evaluate the performance and known limitations of such online service, product or feature for the purposes of such profiling; (6) a description of any transparency measures taken concerning such online service, product or feature with respect to such profiling, including, but not limited to, any measures taken to disclose to consumers that such online service, product or feature is being used for such profiling while such online service, product or feature is being used for such profiling; and (7) a description of the post-deployment monitoring and user safeguards provided concerning such online service, product or feature for the purposes of such profiling, including, but not limited to, the oversight, use and learning processes established by the processor to address issues arising from deployment of such online service, product or feature for the purposes of such profiling.

(c) Each processor that conducts an impact assessment pursuant to subsection (b) of this section shall: (1) Review such impact assessment as necessary to account for any material change to the profiling operations of the online service, product or feature that is the subject of such impact assessment; and (2) maintain documentation concerning such impact assessment for the longer of (A) the three-year period beginning on the date on which such profiling operations cease, or (B) as long as such processor offers such online service, product or feature.

(d) A single impact assessment may address a comparable set of profiling operations that include similar activities.

(e) If a processor conducts an impact assessment for the purpose of complying with another applicable law or regulation, the impact assessment shall be deemed to satisfy the requirements established in this section if such impact assessment is reasonably similar in scope and effect to the impact assessment that would otherwise be conducted pursuant to this section.

(f) If any processor conducts an impact assessment pursuant to subsection (b) of this section and determines that the online service, product or feature that is the subject of such assessment poses a heightened risk of harm to minors, such processor shall establish and implement a plan to mitigate or eliminate such risk. The Attorney General may require a processor to disclose to the Attorney General a plan established and implemented pursuant to this subsection if the plan is relevant to an investigation conducted by the Attorney General.

(g) Impact assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200. To the extent any information contained in an impact assessment disclosed to the Attorney General includes information subject to the attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

[(b)**]** (h) A contract between a controller and a processor shall satisfy the requirements established in subsection (b) of section 42-521.

[(c)**]** (i) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in sections 42-529 to 42-529e, inclusive, as amended by this act.

[(d)**]** (j) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based

determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under section 42-529e.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2025*	New section
Sec. 2	*October 1, 2025*	42-529
Sec. 3	*October 1, 2025*	42-529a
Sec. 4	*October 1, 2025*	42-529b
Sec. 5	*October 1, 2025*	42-529c

GL *Joint Favorable Subst.*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact: None

Municipal Impact: None

Explanation

The bill makes various changes for social media platforms and online services resulting in no fiscal impact to the state. The Office of the Attorney General regulates this area and has the resources and expertise to meet the requirements of the bill.

The Out Years

State Impact: None

Municipal Impact: None

OLR Bill Analysis

sSB 1295

AN ACT CONCERNING SOCIAL MEDIA PLATFORMS AND ONLINE SERVICES, PRODUCTS AND FEATURES.

SUMMARY

This bill adds new protections for minors using social media platforms by requiring platform owners, by January 1, 2026, to incorporate an online safety center and create a policy for handling cyberbullying reports on the platform.

The bill also expands the Connecticut Data Privacy Act to include greater safeguards for minors, including additional factors for controllers (entities that determine the purpose and means of processing personal data) with consumers under age 18 (minor consumers) to (1) use reasonable care to avoid causing harm and (2) conduct a data protection assessment to address these harms and correct the risk. The bill also, among other things,

1. changes the knowledge standard for whether a consumer is a minor for certain requirements and restrictions;

2. prohibits controllers from taking certain actions (e.g., processing a minor's personal data for targeted advertising and personal data sales), by eliminating the option for consent;

3. prohibits direct messaging unless there is a safeguard that prevents unconnected adults from sending unsolicited communications to a minor and requires this to be the default setting; and

4. requires an impact assessment for controllers or processors that do any profiling based on a minor consumer's personal data.

The bill makes various other minor, technical, and conforming changes.

EFFECTIVE DATE: October 1, 2025

§ 1 — SOCIAL MEDIA PLATFORM OWNER REQUIREMENTS

Online Safety Center

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

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

2. access to online behavioral health educational resources;

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

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

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

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

2. enables a user to (a) construct a public or semi-public profile to sign into and use the service or application; (b) populate a public list of other users with whom the user shares a social connection within the service or application; and (c) create or post content seen by other users, including on message boards, in chat rooms,

or through a landing page or main feed that also presents content from other users.

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

1. only provides e-mail or direct messaging;

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

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

Cyberbullying Policy

The bill similarly requires each social media platform owner, by January 1, 2026, to establish a cyberbullying policy with a process for the owner to handle reports of unwanted and aggressive behavior on the platform.

§§ 2-5 — MINORS AND ONLINE SERVICES, PRODUCTS, AND FEATURES

The bill expands the Connecticut Data Privacy Act to:

1. include additional factors for what is considered "heightened risk of harm;"

2. change the standard for certain requirements and restrictions from (a) a willful disregard of knowing the consumer is a minor to (b) knowledge that the consumer is a minor is fairly implied based on objective circumstances;

3. explicitly prohibit controllers that offer an online service, product, or feature to minors from taking certain actions (e.g., processing personal data for targeted advertising and personal data sales) by eliminating the option to consent;

4. prohibit direct messaging unless the controller allows a minor or a minor's parent or legal guardian to prevent adults that the minor is not connected to from sending unsolicited communications and makes this the default setting;

5. explicitly prohibit design features that significantly increase usage; and

6. require an impact assessment for any controller or processor that offers an online service, product, or feature to a minor that does any profiling based on the consumer's personal data.

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

Heightened Risk of Harm to Minors (§§ 2-5)

Existing law requires a controller with minor consumers to use reasonable care to avoid causing any heightened risk of harm to minors in processing personal data. The bill broadens what constitutes "heightened risk of harm to minors" to also include the foreseeable risk of the following:

1. anxiety or depressive disorder, where the disorder has objectively verifiable and clinically diagnosable symptoms and is related to a minor's compulsive use of any online service, product, or feature;

2. compulsive use of any online service, product, or feature;

3. physical violence;

4. harassment on any online service, product, or feature, where it is so severe, pervasive, or objectively offensive that it impacts one or more major life activities;

5. sexual abuse or sexual exploitation;

6. unlawful distribution or sale of, or any consumption or use of, any alcoholic beverage, cannabis, cigarette, e-cigarette, THC-infused beverage, moderate-THC hemp product, narcotic substance, tobacco product, or vapor product; or

7. unlawful gambling.

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

Knowledge Requirement (§§ 3 & 4)

The Connecticut Data Privacy Act currently has several requirements and prohibitions that apply when a controller has actual knowledge, or willfully disregards knowing, that the consumer is a minor. The bill changes the standard for when these requirements and prohibitions apply, from (1) the actual knowledge or willful disregard standard to (2) one of knowledge fairly implied based on objective circumstances. So, when is actual knowledge or knowledge that a consumer is a minor is fairly implied based on the objective circumstances, controllers that offer any online service, product, or feature to consumers who are minors must:

1. use reasonable care to avoid any heightened risk of harm to them;

2. not (a) take certain actions (e.g., processing data for certain purposes); (b) collect precise geolocation data; or (c) provide certain consent mechanisms that are designed to impair user autonomy, among other things; and

3. do a data protection assessment for the online service, product, or feature.

Consent Provision Eliminated (§ 3)

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

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

1. processing any minor's personal data for targeted advertising and personal data sales, profiling to further certain automated decisions (see below), or collect the minor's precise geolocation; and

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

Unsolicited Communications to Minors (§ 3)

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

Features Designed to Increase Use (§ 3)

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

Educational Exception. The bill allows an educational entity,

including a learning management system or a student engagement program, to use a service or application designed to significantly increase, sustain, or extend the use of the online service, product, or feature.

Impact Assessment (§§ 4 & 5)

The bill requires an impact assessment for any controller or processor that offers any online service, product, or feature to a minor if it does any profiling based on the consumer's personal data. They must do these assessments if they have actual knowledge, or have knowledge fairly implied based on objective circumstances, that the consumer is a minor. It requires a processor to provide any information that is needed for a controller to conduct and document an impact assessment.

As under existing law, "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.

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

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

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

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

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

5. any metrics used to evaluate the performance and known limitations of the online service, product, or feature for the profiling;

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

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

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

Review and Retention. The controller or processor, as applicable, must (1) review the assessment as needed to account for any material change to the profiling operations of the online service, product, or feature that is the subject of the assessment and (2) keep documentation on the assessment for the longer of (a) three years, beginning when the profiling operation ends or (b) as long as the service, product, or feature is offered.

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

Plan to Mitigate or Eliminate Risk. Additionally, for controllers or processors with assessments that show their online service, product, or

feature poses a heightened risk to minors, the bill requires them to make and implement a plan to mitigate or eliminate the risk.

The bill also allows the attorney general to require a controller or processor to disclose to him a plan to mitigate or eliminate the risk, for both data protection assessments and impact assessments, if the plan is relevant to an attorney general investigation.

Exempt From Disclosure. Under the bill, impact 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 waive the privilege or protection.

BACKGROUND

Related Bills

sSB 1356, favorably reported by the General Law Committee, among other things, has similar provisions on (1) changing the knowledge standard for determining if a consumer is a minor and (2) prohibiting controllers that offer an online service, product, or feature to minors from taking certain actions, by eliminating the option to consent.

sHB 6857 (File 348), favorably reported by the General Law Committee, among other requirements for platforms, requires a default setting to only allows users connected to a minor to view or respond to content the minor posts.

HB 5474 (File 184), favorably reported by the Committee on Children, has similar provisions on (1) requiring platform owners to incorporate an online safety center and establish a cyberbullying policy for handling reports on the platform, (2) preventing unconnected adults from sending unsolicited messages to minors, (3) prohibiting features designed to increase usage, and (4) an educational exemption.

COMMITTEE ACTION

General Law Committee

Joint Favorable Substitute
Yea 21 Nay 0 (03/21/2025)