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)