August 2, 2023

Analysis of CT SB 3 - An Act Concerning Online Privacy, Data, and Safety Protections.

Executive Summary

On June 26, 2023, Governor Ned Lamont (D) signed SB 3, which enacted additional data privacy privacy and safety protections for minors as well as for consumer health data. The additional requirements related to consumer health data will go into effect on July 1, 2023, while the provisions pertaining to minors' online safety go into effect on October 1, 2024.

The health data provisions implemented include:

- Amending the definition of "sensitive data" included in the Connecticut Data Privacy Act (CTDPA) to include health data;
- Requiring controllers to obtain consumer consent prior to selling or processing a consumer's health data.

The new provisions pertaining to minors' online safety include:

- Prohibitions on processing a minor's personal data for purposes of targeted advertising;
- Prohibitions on the sale of a minors' personal data;
- Prohibitions on collecting a minors' geolocation data;
- Prohibition on using system design features to "significantly increase" a minor's use of an online offering;
- Requiring controllers to conduct data protection assessments regarding the processing of minors' personal data.

Enforcement of these new provisions is carried out exclusively by the Attorney General. A more detailed analysis of the laws' key components is included below.

SB 3 - Consumer Health Data

Effective Date	July 1, 2023; however the minors' online safety provisions do not go into effect until October 1, 2024.
Key Definitions - Health Data	"***Consumer health data***": any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data. ***"Consumer health data controller"***: any controller that, alone or jointly with others, determines the purpose and means of processing consumer health data. ***"Sensitive data"***: personal data that includes (a) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (b) consumer health data, (c) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (d) personal data collected from a known child, (e) data concerning an individual's status as a victim of crime, as defined in section 1-1k, or (f) precise geolocation data.

Key Provisions - Health Data	**Inclusion of consumer health data in the definition of "sensitive data".** Amends the CTDPA's definition of "sensitive data" to include consumer health data. As a result, consumer health data will be subject to the CTDPA's requirement that controllers obtain consumer consent before processing such data. **Prohibition on geofencing** Prohibits the use of geofences near mental, reproductive, and sexual health facilities "for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data." **Prohibition on the sale of consumer health data without consent** Prohibits controllers are prohibited from selling consumer health data without the consumer's consent, similar to the restrictions placed around the processing of consumer health data.
Enforcement	As the section pertaining to consumer health data is being folded into the CTDPA, the enforcement of this section is solely handled by the Attorney General's office. Between July 1, 2023 and December 31, 2024, prior to initiating any action for a violation of this section, the Attorney General's office must "issue a notice of violation to the controller or consumer health data controller if the Attorney General determines that a cure is possible. If the controller or consumer health data controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section."

SB 3 - Minors' Online Safety

Effective Date	July 1, 2023; however the minors' online safety provisions do not go into effect until October 1, 2024.
Key Definitions - Minors' Online Safety	***"Social media platform"***: a public or semi-public internet-based service or application that is used by a consumer in Connecticut, is primarily intended to connect and allow users to socially interact within such service or application, and enables a user to construct a public or semi-public profile for the purposes of signing into and using such service or application, populate a public list of other users with whom the user shares a social connection within such service or application, and create or post content that is viewable by other users, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users. The term does NOT include: (a) a public or semi-public internet-based service or application that exclusively provides electronic mail or direct messaging services, (b) news, sports, entertainment, interactive video games, electronic commerce or content that is preselected by the provider or for which any chat, comments or interactive functionality is incidental to, directly related to, or dependent on the provision of such content, or (c) services used by and under the direction of an educational entity, including, but not limited to, a learning management system or a student engagement program. ***"Minor"***: any consumer who is younger than eighteen years of age. ***"Heightened risk of harm to minors":*** 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.
Key Provisions - Minors Online Safety	**Unpublishing minors' social media accounts** Requires social media companies to "unpublish" – means to remove a social media platform account from visibility – a minors' social media account within 15 business days from receiving such a request from a minor or the minor's parent or legal guardian (if 16 or younger). This provision goes into effect July 1, 2024. **Controller Knowledge Standard** Requires "each controller that offers any online service, product, or feature to consumers with whom such controller has *actual knowledge*, or *wilfully disregards*, are minors shall use reasonable care to avoid any heightened risk of harm to minors caused by such online service, product or feature. **Reasonable care standard** Requires controllers to use reasonable care to avoid any heightened risk of harm to minors caused by their online service, product, or feature. **Restrictions on processing of minor's personal data** Prohibits controllers from processing a minor's personal data for the purposes of targeted advertising, sale of such data, or profiling via automated decision-making systems that produce any legal or similarly significant effect, without consent. Prohibits controllers from processing a minor's personal data unless such processing is necessary to provide the relevant online service, product, or feature, subject to consent exception. **Data protection assessments** Requires controllers to conduct data protection assessments relating to their processing of minors' personal data. **Prohibition on tools designed to increase usage** Prohibits controllers from using "any system design feature to significantly increase, sustain or extend any minor's use of such online service, product or feature." Prohibits controllers from providing any consent mechanism that is "designed to substantially subvert or impair, or is manipulated with the effect of substantially subverting or impairing, user autonomy, decisionmaking or choice[.]" **Geolocation data collection** Prohibits controllers from collecting, without consent, a minor's precise geolocation data, unless it is necessary to provide the relevant feature, time limitation, and that notice is provided to the minor. **Design restrictions for minors** Requires controllers to install limitations on direct messaging apparatuses used by minors, including a limitation on an adult's ability to send direct, unsolicited, messages to a minor. Prohibits controllers from providing any consent mechanism that is "designed to substantially subvert or impair, or is manipulated with the effect of substantially subverting or impairing, user autonomy, decisionmaking or choice[.]"

Enforcement	Enforcement is invested solely with the state Attorney General. Between October 1, 2024 and December 31, 2025, prior to initiating any action for a violation of this section, the Attorney General's office must issue a notice of violation to the controller if the Attorney General determines that a cure is possible. If the controller or consumer health data controller fails to cure such a violation within 60 days of receipt of the notice of violation, the Attorney General may bring an action. Beginning on January 1, 2026, the Attorney General may decide whether or not to provide the controller with a cure period. The bill also establishes that any enforcement provisions brought by the Attorney General for violations of this section, there shall be a rebuttable presumption that a controller used reasonable care as required under the bill if the controller is compliant with the data protection assessment requirements outlined in the bill.