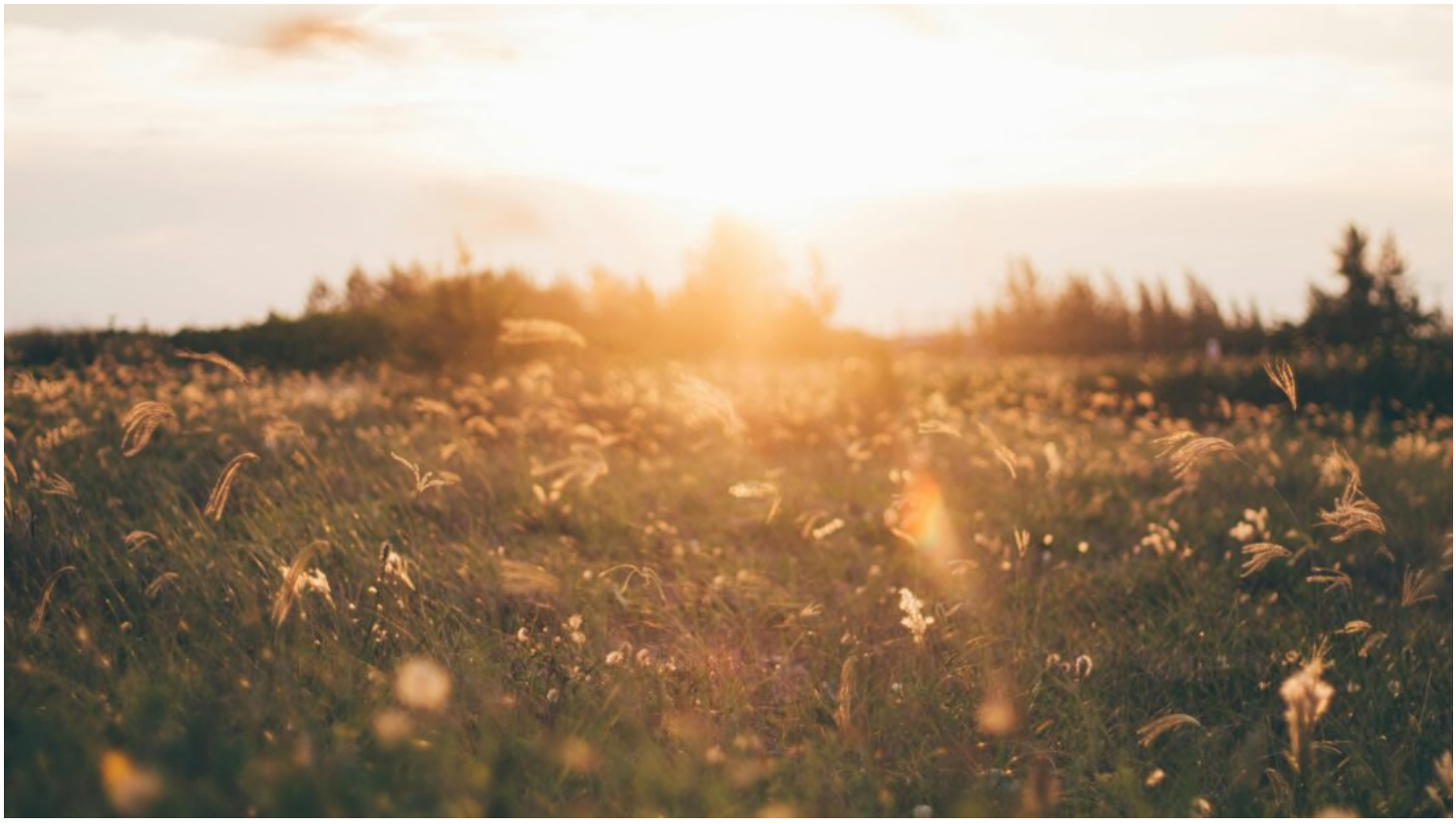
SQUIRE PATTON BOGGS

Privacy World

Keeping you informed on the evolving law on data privacy, security and innovation.

Protecting Kids Online: Changes in California, Connecticut and Congress – Part I



By Julia Jacobson, Alan Friel, Sasha Kiosse & Stacy Swanson on February 27, 2024

Protection for minors online continues to top the list of U.S. regulatory and legislative priorities in 2024. So far in 2024, legislators in California introduced several bills focused on minors; Congress

held hearings and advanced federal legislation protecting minors online; and constitutional challenges to 2023 **state laws** focused on minors' social networking accounts advanced in the Courts. Congress and the Federal Trade Commission (FTC) are looking to update the Children's Online Privacy Protection Act and corresponding Rule, **as detailed in another post**. However, the proposals explained in this post extend far beyond online privacy concerns, and we believe more focus on minors' online safety is on the way.

Because of the complexity of the various efforts to protect children and minors online, we break our analysis into two blog posts. Although approaches differ, we identified some common themes that apply to both Part 1 and Part 2:

- Operators of online services must provide parents, and in some cases, teens, more transparency and control online.
- Age verification is expected. California's proposed laws require that a controller verify age for platforms with addictive features or that serve targeted advertising.
- Additional requirements are proposed for targeted advertising aimed at minors.
- "Addictive" design features and functionality must be assessed and restricted.
- Recommendations algorithms require enhanced transparency, including for adults using a community user-generated content forum.
- Operators of online services must protect the privacy and safety of minors by default.

Not all of these legislative efforts are aimed solely at BigTech: operators of online services of all sizes may face new compliance obligations.

I. CALIFORNIA AND CONNECTICUT

We have previously reported on the **California Age Appropriate Design Act**, which is **being challenged** in court. California is not stopping with that law. On January 29, 2024, California Attorney General Rob Bonta and two California lawmakers introduced two bills: the Social Media Youth Addiction Law (SB 976) and the California Children's Data Privacy Act (AB 1949).

Social Media Youth Addiction Law (SB 976, **available here**): SB 976 requires certain online business to assess and mitigate the potential harms to children due to addictive feeds on social media platforms, including depression, anxiety, and low self-esteem. If enacted, the bill would be added as Chapter 23 to **California's Health and Safety Code**.

Key Definitions

- SB 976 applies to an operator of an "addictive social media platform," which means an online service (including mobile applications) that provides users with an "addictive feed" that is not incidental to the provision of the online service. An "addictive feed" is content "recommended, selected, or prioritized for display" to a user based on information provided by or associated with that user or the user's device, with some exceptions.

Key Prohibitions

- An addictive social media platform is prohibited unless the operator reasonably determines that a user is not a minor (not under age 18) or obtains verifiable parental consent. This prohibition practically requires operators of addictive social media platforms to verify users' ages. The Attorney General is empowered to adopt regulations for age verification.

- The operator of the addictive social media platform also is prohibited from sending notifications to a minor between (in the user's time zone) 12AM and 6AM and between 8AM and 3PM, Monday thru Friday, unless the operator has obtained verifiable parental consent to send the notifications or the parent has modified the default setting using the parental tools described below.

Key Obligations

- *Parental Involvement and Default Settings*: An operator of an addictive social media platform must provide tools through which a "verified parent of a user" may restrict access and use, including:
    - A setting that allows the parent to prevent the minor from accessing or receiving notifications between specific hours;
    - A setting that limits the minor's access to the addictive social media platform to a specific length of time per day, which must be one hour per day by default;
    - A default setting that limits the minor's ability to view feedback (e.g., "likes") within an addictive feed;
    - A default setting of "private mode" for the minor's account so that only other users to whom the minor is connected on the platform may view or respond to the minor's content.
    - A default feed for a minor user is not "recommended, selected, or prioritized for display based on information provided by the user, or otherwise associated with the user of the user's device, other than the user's age or status as a minor."

(Presumably, the verified parent can adjust the default settings.)

- *Annual Reporting*: An operator of an addictive social media platform must annually disclose the number of minor users of its platform and the total number of minors for whom the operator has received verifiable parental consent and to whom the controls above apply.

Regulations

- The Attorney General is empowered to adopt regulations, including specifically for age verification and parental consent.

California Children's Data Privacy Act (AB 1949, **available here**)**:** AB 1949 is a proposed amendment to the California Consumer Privacy Act (CCPA) that applies stricter requirements to a business processing the personal information of minors.

Application and Key Definitions

- As an amendment to CCPA, AB 1949 has the same applicability and defined terms as CCPA (Cal Civ Code 1798.140).

Key Amendments to the CCPA

- The CCPA currently prohibits a business from selling or "sharing" (i.e., disclosures in connection with targeted advertising uses) personal information of a consumer under age 16 "if the business has *actual knowledge* that the consumer is less than 16 years of age, unless the consumer, or the consumer's parent or guardian, as applicable, has affirmatively authorized the sale or sharing of the consumer's personal information" (§ 1798.120(c)).

- AB 1949 eliminates this "actual knowledge" qualifier. Instead, AB 1949 prohibits sale, sharing, collection, use or disclosure of the personal information of consumers under age 18 unless (i) for a consumer age 13 – 17, the business has affirmative authorization of the consumer, or (ii) for a consumer under age 13, a parent or guardian affirmatively authorizes the collection of the consumer's personal information. The practical effect is that the business is responsible for verifying that a consumer is not under age 18 prior to selling, sharing, using, or otherwise disclosing personal information and obtaining affirmative authorization.

Regulations

- AB 1949 requires the California Privacy Protection Agency to adopt regulations regarding age verification and technical specifications for an opt-out preference signal allowing a consumer,

or a consumer's parent or guardian, to specify the minor consumer's age. As part of CCPA, the California Attorney General can seek injunctive relief, damages, or civil penalties of up to $5,000 per violation.

The Attorney General and California lawmakers were likely inspired by **new requirements** added to Connecticut's **consumer privacy law** directed to minors, which means under age 18.

- Effective July 1, 2024, a "social media platform" of any size must remove from public visibility a minor's social media account within 15 business days after receiving a request and must delete a minor's account within 45 business days after receiving a request. The minor account holder or, if the minor is under age 16, the minor's parent may submit the request using the mechanisms described in the social media platform's privacy policy. This section is enforced by the Connecticut Attorney General without a private right of action.
- Effective October 1, 2024, the operator of an "online service" (which is broadly defined) that is offered to a resident of Connecticut who is a known minor (under age 18) or who the operator willfully disregards is a minor must:
    - use reasonable care to avoid "any heightened risk of harm to minor". In the new Connecticut law, "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."
    - NOT deploy any consent mechanism that is designed to "substantially subvert or impair" the decision-making of the minor.
    - NOT make available any direct messaging tools for use by minors without providing readily accessible and easy-to-use safeguards to limit the ability of adults to send unsolicited communications to minors with whom they are not connected.
- Also effective October 1, 2024, a data protection assessment is required when an online service, product or feature is offered to a minor resident of Connecticut. The data protection assessment must address any reasonably-foreseeable heightened risk of harm to minors resulting from the online service, product or feature, among other requirements.

Colorado legislators proposed an **amendment** to the **Colorado Privacy Act** that would add enhanced protections for minor's personal data, requiring controllers to use reasonable care to

avoid any heightened risk of harm to minors. We will provide updates if this amendment is enacted.

In the meantime, please see our table below for a non-inclusive list of other state bills relating to minors and social media use.

II. CONGRESS AND CHILDREN ONLINE

For the past several years, members of Congress have attacked **Section 230** (part of the Communications Decency Act of 1996) as offering protection for online child predators. Section 230 was enacted to help support free speech online by shielding online service operators from the threat of civil liability for content posted by their users. Two Supreme Court cases[1] decided in the first half of 2023 involved the question of immunity under Section 230 but neither case specifically addressed Section 230's scope.

Congress has, however, proposed several laws aimed at limiting Section 230 with respect to online child sexual exploitation and other harms. The two bills currently receiving the most attention are the "Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act of 2023" (**STOP CSAM Act**) and the "Kids Online Safety Act" (**KOSA**), which was first introduced in 2022.

The Hearing

The increased attention to STOP CSAM Act and KOSA is due in no small part to the highly publicized Congressional hearing before the U.S. Senate Judiciary Committee on January 31, 2024, titled "Big Tech and the Online Child Sexual Exploitation Crisis" (the *Hearing*). During the Hearing, the CEOs of five social media platforms testified about their efforts to protect children from sexual exploitation online. The CEOs were grilled by the Judiciary Committee members about the platforms' alleged failure to protect minors from sexually exploitative material and the ineffective tools available to parents for protecting their children from that material.

During the Hearing, one CEO indicated support for the STOP CSAM Act, which was introduced by Dick Durbin (D-IL), Presiding Chair of the Hearing. Other CEOs were more skeptical; one said STOP CSAM Act is "meaningful progress towards eradicating child sexual exploitation from online services" and another said that "parts of the STOP CSAM bill are very encouraging."[2] The Hearing also included testimony from victims of sexual exploitation.

STOP CSAM Act

The STOP CSAM Act has both offline and online measures intended to punish perpetrators of child sexual exploitation and support victims.

The offline measures include special privacy protections and restitution payments for certain child victims and updated sentencing guidelines for perpetrators of child sexual abuse material, as well as mandatory reporting of suspected abuse for non-profits organizations and recipients of federal grants of $10,000+ per year.

The online measures include requirements that "providers", i.e., electronic communication service providers or remote computing service as defined in **Electronic Communications Privacy Act of 1986** (ECPA), report no later than 60 days after obtaining actual knowledge of child porn or other explicit material to **CyberTipline of NCMEC** and penalizing providers that failure to report; and procedures allowing victim to more easily request that providers remove child sexual abuse material and related imagery from their platforms and adding administrative penalties for providers that fail to comply.

KOSA/Amended KOSA

Following the Hearing, an **amended version of KOSA** (Amended KOSA Bill) was released on February 15, 2024. The Amended KOSA Bill has bi-partisan support from **62 co-sponsoring senators** as well as the support of 200+ national and local advocacy groups and experts**.**

Amended KOSA Bill

The Amended KOSA Bill consists of three sections. The first part (Title I) is focused on protecting minors against online material that promotes or creates a heightened risk of compulsive usage, sexual exploitation, online bullying or mental health disorders or other similar risks to minors' physical or mental health (Harms). The much shorter Title III states that the Amended KOSA Bill preempts state law except for a state law that provides greater protection for minors.

Title II – titled "Filter Bubble Transparency" – requires online platforms to provide notice and choice about "opaque algorithms," which means a content ranking system for the online platform that is not based solely on data provided by the user for that purpose. Title II applies to any "any public-facing website, online service, online application, or mobile application that predominantly provides a community forum for user-generated content." (§ 201(6)). This definition means that the opaque-algorithm notice and choice requirement and the rest of Title II apply to more platforms than Title I, which applies only to online platforms *reasonably likely to be used by minors*.

Title I is the longest of the three, consisting of 14 sections that include:

- Covered Platform's Duty of Care: A "covered platform," which is an online service used or "reasonably likely to be used" by minors, must use reasonable care to deploy design features that prevent or mitigate the Harms (§ 102).

- Safeguards for Minors: A covered platform must provide a minor accountholder or visitor with tools to limit or prevent communication, restrict personal data viewing and access, opt out of certain personalized recommendations, delete any account and personal data, and limit the amount of time spent on the covered platform (§ 103(a)).

- Parental Tools: A parent of a minor user must have the ability to view the privacy and account settings, restrict purchases and view time and usage metrics of a minor (under age *17*) and enable by default the ability to change and control privacy and account settings for a child (under age *13*). (§ 103(b)). The covered platform must notify a user when and which parental tool settings apply to the minor users account (§ 103(b)(4)).

- Reporting: Parents, minors, and schools must have an easy and accessible means for reporting "harms to a minor" to the covered platform (§ 103(c)).

- Notice and Transparency: Notice requirements include pre-registration notices to minors about safeguards for minors, personal data use and "personalized recommendation system" use and an overview of how the personalized recommendation system works and how minors or their parents can control or opt out of personalized recommendations in the "terms and conditions" that apply to the covered platform. For children, the notice and verifiable parental consent requirements of the Children's Online Privacy Protection Act (COPPA) apply to the covered platform. When a covered platform has 10M+ active users and "predominantly" offers a community forum for user generated content, transparency requirements include an annual public report with specific content requirements and a third-party inspection of the reasonably foreseeable risk of Harms posed by the covered platform (§§ 104-105).

- Advertising to Minors: Amended KOSA does not prohibit advertising to minors if the advertising is age-appropriate and not based on the minor's personal data. If the advertising is "aimed" at known minors, Amended KOSA includes notice and transparency requirements which require a covered platform to provide "easy-to-understand labels" and information" about the advertisements (§ 104(c)(1)). The notice must include the name of the advertised product or service and disclosure that the content displayed is an advertisement. For individual-specific advertising to minors, information about why the advertisement is directed to a specific minor also is required. (The term "individual-specific advertising to

minors" means advertising that is directed to a specific minor or a device that is linked or reasonably linkable to the minor based on personal data (including a unique device identifier) or "profiling of a minor or group of minors". The term has an exclusion for contextual advertising, among others.) The covered platform also is prohibited from facilitating alcohol, gambling and tobacco advertising to known minors. Many of the details are left to the FTC which is asked with issuing guidance before Amended KOSA's in-force date, making precisely how Amended KOSA will apply to targeted advertising uncertain.

- Effective Date: The Amended KOSA Bill would become effective 18 months after enactment. During that 18-month period, various federal agencies are expected to undertake studies and issue guidance, including research on the relationship between online platforms and the Harms, guidance for covered platforms on conducting research involving minors, age verification strategies, clarifying what constitutes a "design feature, "compulsive usage" and the meaning of "know", such as when a covered platform knows a user is a minor or child (§§ 106-109).

- The FTC and State Attorneys General would enforce the Amended KOSA Bill. The Amended KOSA Bill does not include a private right of action – a topic that has caused federal privacy laws to stall in Congress.

Also at the federal level, changes to the nearly 25-year-old Children's Online Privacy Protection Act (COPPA) are underway. In a **Notice of Proposed Rulemaking** (December 20, 2023), the FTC seeks to expand COPPA's privacy protections and a bill known colloquially as COPPA 2.0 was proposed on same day (February 15, 2024) as the Amended KOSA Bill. See "**Federal Children's Privacy Requirements to Be Updated and Expanded**" for more on COPPA.

At the local level, cities and other states also are encouraging action on social media platforms and minors. In January, **New York City** issued a public health advisory for "adults who interact with children and youth" about the dangers of social media use to "youth mental health". The advisory recommends that adults implement tech-free times and places; discuss social media use and provide support when youth identify concerns; and model healthy social media use. Below is our non-inclusive list of other state bills relating to minors and social media use.

Watch for Part II, which will focus on how laws aimed at parental control of social media accounts are faring in the courts and other kid-focused updates.

State	Bill re: Minors and Social Media Use	Bill Status
Massachusetts	An act relative to internet privacy rights for children (proposed addition to state consumer protection law as Chapter 93, § 115)	Introduced on February 16, 2023; joint hearing took on October 19, 2023. Reporting date extended to April 8, 2024. (**Track here**)
Pennsylvania	Protecting Minors on Social Media	The bill was "laid on the table" on October 25, 2023, for future consideration. (**Track here**)
New Jersey	• An Act concerning social media privacy and data management standards for children and establishing the New Jersey Children's Data Protection Commission. • An Act prohibiting the use of certain addictive practices or features by social media platforms.	All were carried forward from 2023. • Assembly Bill 1879 / SB 3493 (**Track here** and **here**) • Assembly Bill 1883 / SB 3608 (**Track here** and **here**)
New York	• New York Social Media Regulation Act – relates to the regulation of social media companies and social media platforms; provides for age requirements for the use of social media and parental consent; prohibits certain data collection from social media accounts; limits the hours a minor can have access to social media; establishes penalties for violations. • Child Data Privacy and Protection Act – to prevent the exploitation of children's data; requires data controllers to assess the impact of its products on children; bans certain data collection and targeted advertising.	• The New York Social Media Regulation Act was re-referred to committee on January 3, 2024. (**Track here**) • The Child Data Privacy and Protection Act was re-referred to committee on January 3, 2024. (**Track here**)

State	Bill re: Minors and Social Media Use	Bill Status
North Carolina	• Let Parents Choose Protection Act • Social Media Algorithmic Control in IT Act • Social Media Accountability Act	The three bills were introduced in April 2023 and re-referred to committee. • Track the Let Parents Choose Protection Act (**Track here**) • Track the Social Media Algorithmic Control in IT Act (**Track here**) • Track Social Media Accountability Act (**Track here**)
Illinois	• Children's Privacy Protection and Parental Empowerment Act • Minor Online Data Privacy Act.	• The Children's Privacy Protection and Parental Empowerment Act was introduced February 17, 2023, and re-referred to committee on March 10, 2023. (**Track here**) • The Minor Online Data Privacy Act was introduced on February 9, 2023, and referred to committee. (**Track here**)
Maryland	Maryland Kids Code	The Maryland Kids Code was first proposed as the Age-Appropriate Design Code Act (**HB901**) and passed the Maryland House on March 20, 2023 (**discussed in our previous blog post**), but not the Maryland Senate. (Track **HB 603 here** and **SB 571 here**)
Minnesota	**Unlawful Social Media Activities** (prohibiting certain social media algorithms that target children)	Carried over to February 2024 legislative session. (**Track here**)
Vermont	Age-appropriate Design Code	Introduced January 17, 2024. (**Track here**)
West Virginia	Online Privacy Protection for Children – proposed new section for the state's	Introduced January 15, 2024. (**Track here**)

State	Bill re: Minors and Social Media Use	Bill Status
	consumer protection law titled (§ 46A-9-1 et seq)	

Privacy World will continue to cover updates related to these bills and privacy law developments generally. Please contact the authors for more information.

• • • •

Disclaimer: *While every effort has been made to ensure that the information contained in this article is accurate, neither its authors nor Squire Patton Boggs accepts responsibility for any errors or omissions. The content of this article is for general information only and is not intended to constitute or be relied upon as legal advice.*

---

[1] See, e.g., "Section 230 and the Internet", SCOTUS Blog, February 28, 2023, at **https://www.scotusblog.com/2023/02/supreme-court-section-230-and-the-internet/**

[2] See **https://www.durbin.senate.gov/newsroom/press-releases/durbin-presses-big-tech-ceos-to-protect-kids-from-sexual-exploitation-online-during-senate-judiciary-committee-hearing**