SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

SB 1444 (Stern)
Version: February 16, 2024
Hearing Date: April 23, 2024
Fiscal: Yes
Urgency: No
CK

SUBJECT

Let Parents Choose Protection Act of 2024

DIGEST

This bill requires large social media platforms to provide mechanisms for third-party safety software providers to seek transfer of minor users' data and to control the child's online interactions, content, and account settings on the delegation of the child or their parent or guardian.

EXECUTIVE SUMMARY

In 2005, five percent of adults in the United States used social media. In just six years, that number jumped to half of all Americans. Today, over 70 percent of adults use at least one social media platform. Facebook alone is used by 69 percent of adults, and 70 percent of those adults say they use the platform on a daily basis.

However, this explosion is not limited to adults. Survey data found that overall screen use among teens and tweens increased by 17 percent from 2019 to 2021 with the number of hours spent online spiking sharply during the pandemic. A recent survey found almost 40 percent of tweens stated that they used social media and estimates from 2018 put the number of teens on the sites at over 70 percent.

Given the reach of social media platforms and the increasing role they play in many children's lives, concerns have arisen over the connection between social media usage and mental health, drug use, and other self-harming conduct. This bill seeks to address these issues by mandating large social media platforms provide access, through real-time application programing interfaces, to children's accounts and allow these third parties to manage the child's online interactions, content, and account settings. The Attorney General is charged with oversight, enforcement, and promulgating regulations to guide compliance and safety and security.

The bill is sponsored by the Organization for Social Media Safety. It is supported by various organizations, including Mothers Against Prescription Drug Abuse. It is opposed by Oakland Privacy and several industry associations, including the California Chamber of Commerce.

PROPOSED CHANGES TO THE LAW

1) Establishes the Privacy Rights for California Minors in the Digital World (PRCMDW), which prohibits an operator of an internet website, online service, online application, or mobile application ("operator") from the following:
    a) marketing or advertising specified products or services, such as firearms, cigarettes, and alcoholic beverages, on its internet website, online service, online application, or mobile application that is directed to minors;
    b) marketing or advertising such products or services to minors who the operator has actual knowledge are using its site, service, or application online and is a minor, if the marketing or advertising is specifically directed to that minor based upon the personal information of the minor; and;
    c) knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile, the personal information of a minor with actual knowledge that the use, disclosure, or compilation is for the purpose of marketing or advertising such products or services to that minor, where the website, service, or application is directed to minors or there is actual knowledge that a minor is using the website, service, or application. (Bus. & Prof. Code § 22580.)

2) Requires, pursuant to the PRCMDW, certain operators to permit a minor user to remove the minor's content or information and to further inform the minor of this right and the process for exercising it. (Bus. & Prof. Code § 22581.)

3) Requires, pursuant to the Parent's Accountability and Child Protection Act, a person or business that conducts business in California, and that seeks to sell any product or service in or into California that is illegal under state law to sell to a minor to, notwithstanding any general term or condition, take reasonable steps, as specified, to ensure that the purchaser is of legal age at the time of purchase or delivery, including, but not limited to, verifying the age of the purchaser. (Civ. Code § 1798.99.1(a)(1).)

4) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

5) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and creates the California Privacy Protection Agency (PPA), which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

6) Prohibits a business from selling or sharing the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. (Civ. Code § 1798.120.)

7) Permits amendment of the CPRA by a majority vote of each house of the Legislature and the signature of the Governor, provided such amendments are consistent with and further the purpose and intent of this act as set forth therein. (Proposition 24 § 25 (2020).)

8) Establishes the California Age-Appropriate Design Code Act, which places a series of obligations and restrictions on businesses that provide online services, products, or features likely to be accessed by children. (Civ. Code § 1798.99.28 et seq.)

9) Requires a business that provides an online service, product, or feature likely to be accessed by children ("covered business") to take specified actions, including to:
    a) undertake a Data Protection Impact Assessment for any online service, product, or feature likely to be accessed by children, as specified;
    b) estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business, or apply the privacy and data protections afforded to children to all consumers;
    c) provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature;
    d) if the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an obvious signal to the child when the child is being monitored or tracked;

e) enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children; and
f) provide prominent, accessible, and responsive tools to help children, or if applicable their parent or guardian, exercise their privacy rights and report concerns. (Civ. Code § 1798.99.31.)

10) Provides that a covered business shall not engage in specified activity, including:
a) using the personal information of any child in a way that the business knows or has reason to know is materially detrimental to the physical health, mental health, or well-being of a child;
b) profiling a child by default, except as specified;
c) collecting, selling, sharing, or retaining any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, except as specified;
d) using the personal information of a child for any reason other than a reason for which that personal information was collected, except as specified;
e) collecting, selling, or sharing any precise geolocation information of children by default unless the collection of that precise geolocation information is strictly necessary to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature; and
f) collecting, selling, or sharing any precise geolocation information without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected. (Civ. Code § 1798.99.31.)

This bill:

1) Requires a "large social media platform provider," before August 1, 2025, or within 30 days after a service becomes a large social media platform, as applicable, to create, maintain, and make available to any third-party safety software provider registered with the Attorney General a set of third-party-accessible real time application programming interfaces (APIs), including any information necessary to use the interfaces, by which a child, or a parent or legal guardian of a child, may delegate permission to the third-party safety software provider to do the following:
a) Manage the child's online interactions, content, and account settings on the large social media platform.
b) Initiate secure transfers of user data from the large social media platform in a commonly used and machine-readable format to the third-party safety software provider, and the frequency of the transfers may not be

limited by the large social media platform provider to less than once per hour.

2) Provides that once a child or a parent or legal guardian of a child makes a delegation, the provider shall make the APIs and information available to the third-party safety software provider on an ongoing basis until one of the following applies:
    a) The delegation is revoked by the child or the child's parent or legal guardian.
    b) The child's account is disabled with the large social media platform.
    c) The third-party safety software provider rejects the delegation.
    d) One or more of the affirmations made by the third-party safety software provider in connection with registration is no longer true.

3) Requires platforms to establish and implement reasonable policies, practices, and procedures regarding the secure transfer of user data pursuant to a delegation from the large social media platform to a third-party safety software provider in order to mitigate any risks related to user data.

4) Provides that if a delegation is made, the provider must do all of the following:
    a) Disclose to the child, and the parent or legal guardian if they made the delegation, the fact that the delegation has been made.
    b) Provide to the child, and the parent or legal guardian if they made the delegation, a summary of what user data is being transferred to the third-party safety software provider, along with updates if the data being collected changes.

5) Prohibits a third-party safety software provider from disclosing any user data obtained under this section to any person except as follows:
    a) Pursuant to a lawful request for law enforcement purposes or for judicial or administrative proceedings by means of a court order or a court ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.
    b) To the extent that the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of that law.
    c) To the child, or a parent or legal guardian of the child, who made a delegation and whose data is at issue. The disclosure shall be limited, by a good faith effort on the part of the third-party safety software provider, only to the user data strictly sufficient for a reasonable parent or legal guardian to understand that the child is at foreseeable risk or currently experiencing any of the following harms:
        i. Suicide.
        ii. Anxiety.
        iii. Depression.

iv. Eating disorders.
v. Violence, including being the victim of or planning to commit or facilitate battery and assault, as defined.
vi. Substance abuse.
vii. Fraud.
viii. Human trafficking.
ix. Sexual abuse.
x. Physical injury.
xi. Harassment, including hate-based harassment, sexual harassment, and stalking.
xii. Exposure to "harmful matter."
xiii. Communicating with a terrorist organization.
xiv. Academic dishonesty, including cheating, plagiarism, or other forms of academic dishonesty that are intended to gain an unfair academic advantage.
xv. Sharing personal information, including address, telephone number, social security number, and banking information.

d) In the case of a reasonably foreseeable serious and imminent threat to the health or safety of any individual, if the disclosure is made to a person or persons reasonably able to prevent or lessen the threat.

6) Requires the platform to notify the child user and parents that any such disclosure has been made.

7) Requires third-party safety software providers to register with the Attorney General's office in order to get access to the APIs. The provider must affirm they are solely engaged in business of internet safety, will only use the data to protect children from harm, will only disclose the data as permitted, and will provide clear disclosures to parents. Any changes must be reported to the Attorney General and the child or parent.

8) Authorizes the Attorney General to deregister or issue a civil penalty not to exceed $5,000 per violation to a third-party safety software provider if it is determined that the provider has violated or misrepresented the affirmations made or has not properly disclosed a change to an affirmation as required. The Attorney General must notify platforms when it deregisters any providers.

9) Requires large social media platforms to register with the Attorney General, as provided.

10) Provides that in any civil action, other than an action brought by the Attorney General, a large social media platform provider shall not be held liable for damages arising out of the transfer of user data to a third-party safety software provider in accordance with this chapter, if the large social media platform

provider has in good faith complied with the requirements of this chapter and the guidance issued by the Attorney General in accordance with this act.

11) Requires the California Department of Technology (CDT), before July 1, 2025, to issue guidance for platform providers and third-party safety software providers regarding the implementation and maintenance of technical standards to protect user data based on a review of prevailing industry practices and technical safeguards published by the National Institute of Standards and Technology (NIST). CDT is required to update the guidance biennially.

12) Requires the Attorney General to administer and enforce this law and to issue guidance, before July 1, 2025, on both of the following:
    a) Facilitating a third-party safety software provider's ability to obtain user data or access in a way that ensures that a request for user data or access on behalf of a child is a verifiable request.
    b) For large social media platform providers and third-party safety software providers, maintaining reasonable safety standards to protect user data.

13) Requires the Attorney General to make publicly available on the website a list of the registered third-party safety software providers, a list of the registered large social media platforms, and a list of the third-party safety software providers deregistered.

14) Authorizes the Attorney General to adopt emergency regulations to implement this chapter.

15) Defines the relevant terms, including:
    a) "Large social media platform" means, except as provided, a service that meets all of the following:
        i. Is provided through an internet website or a mobile application, or both.
        ii. The terms of service do not prohibit the use of the service by a child.
        iii. The service includes features that enable a child to share images, text, or video through the internet with other users of the service whom the child has met, identified, or become aware of solely through the use of the service.
        iv. The service has more than 100,000,000 monthly global active users or generates more than $1 billion in gross revenue per year, adjusted yearly for inflation, or both.
    b) "Third-party safety software provider" means any person who, for commercial purposes, is authorized by a child, if the child is 13 years of age or older, or a parent or legal guardian of a child, to interact with a large social media platform to manage the child's online interactions,

content, or account settings for the sole purpose of protecting the child from harm, including physical or emotional harm.

16) Provides an operative date of July 1, 2025.

17) Provides that the Legislature finds and declares that this act furthers the purposes and intent of the California Privacy Rights Act of 2020.

COMMENTS

1. Social media and children

The effects of social media on our mental health and what should and can be done about it are pressing policy and societal questions that have become increasingly urgent. Evidence shows that engagement on social media has a clear effect on our emotions.

Researchers conducted a massive experiment on Facebook involving almost 700,000 users to test the emotional effects of social networks:

> The results show emotional contagion. [For] people who had positive content reduced in their News Feed, a larger percentage of words in people's status updates were negative and a smaller percentage were positive. When negativity was reduced, the opposite pattern occurred. These results suggest that the emotions expressed by friends, via online social networks, influence our own moods, constituting, to our knowledge, the first experimental evidence for massive-scale emotional contagion via social networks [. . .] and providing support for previously contested claims that emotions spread via contagion through a network.[1]

Research has shown that amongst American teenagers, YouTube, Instagram, and Snapchat are the most popular social media sites, and 45 percent of teenagers stated that they are "online almost constantly."[2] A meta-analysis of research on social networking site (SNS) use concluded the studies supported an association between problematic SNS

---

[1] Adam D. I. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks* (June 17, 2014) Proceedings of the National Academy of Sciences, vol. 111, No. 24, https://www.pnas.org/doi/full/10.1073/pnas.1320040111. All internet citations are current as of April 16, 2024.

[2] Zaheer Hussain and Mark D Griffiths, *Problematic Social Networking Site Use and Comorbid Psychiatric Disorders: A Systematic Review of Recent Large-Scale Studies*." (December 14, 2018) Frontiers in psychiatry vol. 9 686, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6302102/pdf/fpsyt-09-00686.pdf.

use and psychiatric disorder symptoms, particularly in adolescents.[3] The study found most associations were with depression and anxiety.

Another paper recently released provides "Recommendations to the Biden Administration," and is relevant to the considerations here:

> The Administration should work with Congress to develop a system of financial incentives to encourage greater industry attention to the social costs, or "externalities," imposed by social media platforms. A system of meaningful fines for violating industry standards of conduct regarding harmful content on the internet is one example. In addition, the Administration should promote greater transparency of the placement of digital advertising, the dominant source of social media revenue. This would create an incentive for social media companies to modify their algorithms and practices related to harmful content, which their advertisers generally seek to avoid.[4]

A series of startling revelations unfolded after a Facebook whistle-blower, Frances Haugen, began sharing internal documents. The Wall Street Journal published many of the findings:

> About a year ago, teenager Anastasia Vlasova started seeing a therapist. She had developed an eating disorder, and had a clear idea of what led to it: her time on Instagram.
>
> She joined the platform at 13, and eventually was spending three hours a day entranced by the seemingly perfect lives and bodies of the fitness influencers who posted on the app.
>
> "When I went on Instagram, all I saw were images of chiseled bodies, perfect abs and women doing 100 burpees in 10 minutes," said Ms. Vlasova, now 18, who lives in Reston, Va.
>
> Around that time, researchers inside Instagram, which is owned by Facebook Inc., were studying this kind of experience and asking whether it was part of a broader phenomenon. Their findings confirmed some serious problems.

---

[3] *Ibid.*

[4] Caroline Atkinson, et al., *Recommendations to the Biden Administration On Regulating Disinformation and Other Harmful Content on Social Media* (March 2021) Harvard Kennedy School & New York University Stern School of Business, https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/6058a456ca24454a73370dc8/1616421974691/TechnologyRecommendations_2021final.pdf.

> "Thirty-two percent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse," the researchers said in a March 2020 slide presentation posted to Facebook's internal message board, reviewed by The Wall Street Journal. "Comparisons on Instagram can change how young women view and describe themselves."
>
> For the past three years, Facebook has been conducting studies into how its photo-sharing app affects its millions of young users. Repeatedly, the company's researchers found that Instagram is harmful for a sizable percentage of them, most notably teenage girls.
>
> "We make body image issues worse for one in three teen girls," said one slide from 2019, summarizing research about teen girls who experience the issues.
>
> "Teens blame Instagram for increases in the rate of anxiety and depression," said another slide. "This reaction was unprompted and consistent across all groups."
>
> Among teens who reported suicidal thoughts, 13% of British users and 6% of American users traced the desire to kill themselves to Instagram, one presentation showed.
>
> Expanding its base of young users is vital to the company's more than $100 billion in annual revenue, and it doesn't want to jeopardize their engagement with the platform.
>
> More than 40% of Instagram's users are 22 years old and younger, and about 22 million teens log onto Instagram in the U.S. each day . . . .[5]

Cyberbullying—bullying tactics made through online means—is also remarkably prevalent. Studies suggest that around 15 percent of teens and tweens have experienced cyberbullying.[6] Bullying of any kind is associated with negative health effects, but cyberbullying presents unique risks to its victims in light of the nature of social media and the internet in general. Social media platforms can be used to create a false profile for a person, disseminate embarrassing photos or videos, or engage in bullying anonymously in ways that are not available in the real world.

---

[5] Georgia Wells et al., *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show* (September 14, 2021) The Wall Street Journal, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=article_inline.

[6] *See* Basile, et al., *Interpersonal Violence Victimization Among High School Students – Youth Risk Behavior Survey, United States, 2019*, CDC National Center for Injury Prevention and Control, Division of Violence Prevention (Aug. 21, 2020), at p. 1; Patchin & Hinduja, *Tween Cyberbullying in 2020*, Cyberbullying Research Center (2020) at p. 4.

Another increasing prevalent issue is the connection between social media and drug use in children. Drug use among teenagers and young adults has surged, in part due to the mental health harms caused by the COVID-19 pandemic.[7] Teenagers and young adults appear to prefer using prescription pills over opioids like heroin, due to "a skittishness about syringes" and "the false imprimatur of medical authority" that comes with prescription medication.[8]

For many young people seeking pills, they need look no further than the social media apps on their smartphones. Large numbers of drug dealers now use social media apps—particularly those with encrypted or disappearing messages—to offer drugs and make sales.[9] Snapchat, a social media app with features that allow messages to disappear and to be locked with a password, has been particularly widely criticized for facilitating drug sales to minors over its platform,[10] but the DEA has identified other social media platforms—including Facebook, Instagram, and TikTok—that are also used for drug sales.[11] Drug dealers have been able to exploit the built-in features of these platforms, as well as inconsistent content moderation by the platforms, to the point that "gaining access to illicit drugs via social media…is nearly as convenient as using one's phone to order a pizza or call an Uber."[12]

Representatives from Snap (Snapchat's parent company) and other social media companies say that they have taken steps to identify drug dealer accounts and limit the sales of drugs on their platforms.[13] Some argue, however, that the steps are inadequate to meaningfully reduce the problem.[14] Others report that social media platforms have been slow to cooperate with law enforcement officials investigating drug sales arranged over the platforms, further thwarting efforts to protect minors.[15] In February 2023, the

---

[7] Hoffman, *Fentanyl Tainted Pills Bought on Social Media Cause Youth Drug Deaths to Soar* (May 19, 2022) N.Y. Times, https://www.nytimes.com/2022/05/19/health/pills-fentanyl-social-media.html.
[8] *Ibid.*
[9] *Ibid.*; Whitehurst, *Group urges feds to investigate Snapchat over fentanyl sales* (Dec. 22, 2022) L.A. Times, https://www.latimes.com/business/story/2022-12-23/group-urges-feds-investigate-snapchat-over-fentanyl-sales.
[10] Mann, *Social media platforms face pressure to stop online drug dealers who target kids* (Jan. 26, 2023) NPR, https://www.npr.org/2023/01/26/1151474285/social-media-platforms-face-pressure-to-stop-online-drug-dealers-who-target-kids.
[11] Whitehurst, *Group urges feds to investigate Snapchat over fentanyl sales* (Dec. 22, 2022) L.A. Times, https://www.latimes.com/business/story/2022-12-23/group-urges-feds-investigate-snapchat-over-fentanyl-sales.
[12] Colorado Department of Law, *Social Media, Fentanyl, & Illegal Drug Sales: A Report from the Colorado Department of Law* (2023), pp. 8-9.
[13] Mann, *Social media platforms face pressure to stop online drug dealers who target kids* (Jan. 26, 2023) NPR, https://www.npr.org/2023/01/26/1151474285/social-media-platforms-face-pressure-to-stop-online-drug-dealers-who-target-kids; Hoffman, *Fentanyl Tainted Pills Bought on Social Media Cause Youth Drug Deaths to Soar* (May 19, 2022) N.Y. Times, https://www.nytimes.com/2022/05/19/health/pills-fentanyl-social-media.html.
[14] Colorado Department of Law, *Social Media, Fentanyl, & Illegal Drug Sales: A Report from the Colorado Department of Law*, *supra* at p. 7.
[15] *Id.* at p. 87.

House Energy and Commerce Committee held a roundtable to discuss the problem of drug sales over social media and whether federal legislation is needed to limit the liability protections given to online platforms for injuries caused by drug sales facilitated by those platforms.[16]

2. Looking to third-party safety software providers for help

This bill seeks to address these issues by making it easier for certain companies, third-party safety software providers, to get transfers of a child users' data and the ability to manage all of the child's online interactions, content, and account settings on a social media platform. The bill requires the social media platforms to create and maintain an API that it makes accessible to these third party providers on an ongoing basis and provide instructions on how to use them. The third party providers can then have parents of these child users delegate authority to the providers to manage the child's online activities and download all of the child's data from the platform.

Once the information is in the control of the third-party providers, the bill places certain restrictions on whom they can disclose the information to. This includes to law enforcement and in response to subpoenas. The providers can disclose the information to parents, but they are required to make a "good faith effort" to limit the information disclosed to them only to the data "strictly sufficient for a reasonable parent or legal guardian to understand that the child is at foreseeable risk or currently experiencing" specified harms, including things such as depression, substance abuse, exposure to harmful matter, or sharing their contact information.

According to the author:

> One of the most effective ways for parents to protect children is by using third-party safety apps. These apps can provide alerts to parents when dangerous content is shared through children's social media accounts, enabling life-saving interventions at critical moments. For example, if a child is expressing thoughts of suicide via social media, then a parent, who has received an alert through a third-party safety app, can immediately provide mental health support. We know from the data that these alerts have already protected hundreds of thousands of children.
>
> For third-party safety apps to work, the social media companies need to give them permission. While many social media platforms do provide this access, unfortunately, other major platforms, do not, even though the burden on the platforms of providing access is negligible and can be done

[16] Feiner, *Snaptchat's role in fentanyl crisis probed during house roundtable: "It's a Snap-specific problem'* (Jan. 25, 2023) CNBC, https://www.cnbc.com/2023/01/25/snapchats-role-in-fentanyl-crisis-probed-during-house-roundtable.html.

> securely using existing, industry-standardized technology. To save lives, parents need to be the ones who make the choice about whether they want to use third-party safety apps.
>
> Sammy's Law requires that, upon request by a parent of a child account holder, large social media platforms will transfer the child's data to the registered third-party safety software provider chosen by the parent. This data access will enable the safety software to provide alerts to the parent when dangerous content is shared on or through a child's account.
> The extent of harm that social media is inflicting upon children is ongoing, pervasive, and severe. Despite rising awareness of this harms over recent years and various legislative efforts, the risk to children's health and welfare from social media use continues. Third-party safety software is an existing, proven solution to rapidly increase safety for young adult social media users. California has a compelling governmental interest in ensuring that parents can at least choose to use these additional safety tools given the harm that is happening under the status quo.

The Organization for Social Media Safety, the sponsor of this bill, writes in support:

> Social media platforms face real constraints on their capacity to maximize safety, and they simply cannot replicate the significant, additional protections that third-party safety software can provide. If a child expresses thoughts of suicide on social media, social media platforms are simply not situated to provide immediate interventions. Social media platforms are often unable to detect severe and repeated cyberbullying without a report from a user. Even when they do detect it, the platforms cannot provide the immediate, necessary supports to the child, like a parent or guardian can. Despite seemingly significant efforts on the part of platforms, sexual predators continue to target children on social media. And even though platforms have announced in recent years new measures to combat drug traffickers, dealers continue to operate on various platforms. That is likely why Snap Inc.'s representative said in an October 26, 2021, Senate Commerce Committee hearing, "We have employed proactive detection measures to get ahead of what the drug dealers are doing. They are constantly evading our tactics, not just on Snapchat but on every platform." Third-party safety software not only detects these threats more effectively than the platforms, but also provides immediate, life-saving alerts to parents or guardians.

3. Concerns with this model

A number of concerns have been raised in response to the approach taken by this bill. First, there are privacy concerns as the bill envisions near constant data sharing, which involves the personal information of children, including highly sensitive information. Platforms are specifically prohibited from limiting the frequency of the transfers to less than once per hour. Given the political and legal climate in other parts of the country, user data that reveals details about reproductive or gender-affirming health care, for instance, could open up these children and even their families to legal liability. Even with the limitations in the bill on disclosure, authorities in other states could subpoena that information to enforce laws that are incongruent with California's values. The bill provides a finding that this bill "furthers the purposes and intent of the California Privacy Rights Act of 2020." However, the expansive transfers of personal information to private companies enabled by this bill may arguably fail to meet that standard.

In addition, while many parents will use providers such as these for monitoring social media to ensure they are being safe, some families are not as supportive of their children. For instance, a teen that is struggling with a lack of acceptance of their sexuality or gender identity might look to social media for support and resources, only to have that information provided to parents that might not be supportive. A nearly identical bill is being considered in Illinois, with groups such as Equality Illinois, ACLU of Illinois, and Planned Parenthood Illinois Action all in opposition for these reasons.

Another concern is focused on security. The bill does require platforms to implement reasonable procedures for these transfers and CDT is required to issue guidance for implementation and maintenance of technical standards to protect the data. However, there is a measure of immunity provided to the platforms offloading the data in connection with damages arising out of those very transfers:

> In any civil action, other than an action brought by the Attorney General, a large social media platform provider shall not be held liable for damages arising out of the transfer of user data to a third-party safety software provider in accordance with this chapter, if the large social media platform provider has in good faith complied with the requirements of this chapter and the guidance issued by the Attorney General in accordance with this act.

The Attorney General is also required to issue guidance, specifically on ensuring that a data or access request on behalf of a child is a verifiable request. This is eminently critical to protecting children given what is in play. There are concerns that a tool such as that provided by the bill could enable domestic abusers, stalkers, or other bad actors to gain access over and surveil a child's account, or even an adult victim.

The sponsor of this bill, the Organization for Social Media Safety, writes:

> Sammy's Law would also not be a burden to the social media platforms or weaken data security. In terms of set-up and ongoing operations, established social media platforms face negligible burdens in providing third-party safety software the ability to access data, with parental consent. The mechanism by which this data would be shared between the social media platform and third-party safety app, an application programming interface (API), is standard in the industry. In fact, APIs currently facilitate the interactions between social media software and the server for all major social media platforms whether or not the platform offers data access to third-party safety software. APIs are also used by millions across the world daily to transfer sensitive information, like financial and health data, between applications.

Writing in opposition, the Computer and Communications Industry Association emphasizes these concerns:

> SB 1444 would effectively create a framework under which a third-party vendor would be able to amass a significant amount of personal information about users under 18 across many service types. This creating and storing of such a vast amount of data by a vendor about this younger population inherently raises concerns about the security practices of those third-party vendors.
>
> The bill also raises security concerns with regard to requiring private companies to make their application programming interfaces (APIs) accessible to third parties. Generally, APIs that are maintained internally are subject to a greater level of protection, through several layers of security. Opening up the level of accessibility would pose additional risks.
>
> Recent studies have also sparked concerns at the federal level. In 2021, Senators Elizabeth Warren (D-MA), Edward J. Markey (D-MA), and Richard Blumenthal (D-CT) submitted a letter to the Chief Executive Officer of Bark Technologies, Inc.,[17] outlining significant concerns about how the software may be "surveilling students inappropriately" and "compounding racial disparities in school discipline." While the letter focuses on negative impacts of using such "surveillance" software in an educational setting, the concerns extend beyond that – it boils down to the fundamental issue that this third-party software allows for the tracking and surreptitious control of nearly all of a child's online behavior.

[17] It should be noted that Bark Technologies is a supporter of this bill.

Another concern is the vetting of which third party providers are allowed access to these APIs. The providers must register with the Attorney General and make certain affirmations. The provider must affirm they are solely engaged in the business of internet safety, will only use the data to protect children from harm, will only disclose the data as permitted, and will provide clear disclosures to parents.

A coalition of groups in opposition, including Technet, explain:

> [T]here seem to be very few requirements to be a third-party software provider apart from five short affirmations. Additional vetting and requirements are required to just match the current standard that platforms require of third-party providers. In this way SB 1444 rolls back industry standards that are already in place by requiring platforms to provide an API to any third-party software provider and removing platforms' discretion. This could jeopardize both user data and platforms' intellectual property.
>
> SB 1444 is also vague as to the service provided by third-party software providers. The bill allows a third-party provider to "manage the child's online interactions, content, and account settings" and "initiate secure transfers of user data" from a social media company to a third-party provider. There are no requirements in SB 1444 that a third-party provider must maintain a platform's own safety and privacy settings for minors. At a minimum, a third-party should not be able to unwind the many settings, features, parental controls, policies, and protections platforms have created to ensure a safe environment for teen users.

4. Additional stakeholder positions

D.A.R.E. America writes in support:

> SB 1444 finds the right balance between preserving privacy and protecting children from social media-related harms. It requires that, upon request by a parent of a child account holder, large social media platforms will transfer the child's data to the registered third-party safety software provider chosen by the parent. This data access is what enables the safety software to provide alerts to the parent when dangerous content is shared on or through a child's account. SB 1444 further requires that third-party safety software providers may only disclose to the parent or guardian data relevant and connected to specific risks threatening the health and safety of a child.
>
> Social media platforms suggest that they have the capability to maximize child safety themselves. The status quo indicates otherwise. Despite some

> platforms even announcing new safety features and policies over the past few years, the pervasive, severe harm to children continues.

A coalition of industry associations, including NetChoice, argues in opposition:

> SB 1444 requires large social media platforms to make an application programming interface (API) available to a third-party software provider, removing all discretion from those companies. Currently, companies can decide who they provide an API to and condition the use of that API as appropriate. Third-parties are thoroughly vetted prior to any agreement to determine their ability to secure user and platform data and prevent data breaches. Platforms can also restrict access to certain parts of the platform as well as restrict and condition the use of different types of user data. Many of these agreements are formalized with contracts and provide clear remedies if intellectual property is misappropriated or if user data is breached. SB 1444 removes platforms' abilities to negotiate their contracts with third-party software providers and forces platforms to provide an API.

The Drug Induced Homicide Organization writes in support:

> Unfortunately, despite the minimal burden on platforms to provide such access, which can be securely facilitated using existing, industry-standard technology, not all companies have been cooperative. Platforms like Snapchat and TikTok, frequented by millions of young users, have yet to offer the necessary permissions for third-party safety software to function effectively. Sammy's Law will address this gap, ensuring that all platforms, without exception, offer parents the option to safeguard their children through these technological means.
>
> The provision of this choice to parents is not just about enhancing safety measures; it is about affirming the role of parents in protecting their children in an ever-evolving digital landscape. It acknowledges the importance of parental guidance and the right of parents to employ all available tools to ensure their children's wellbeing.

The Computer & Communications Industry Association writes in opposition:

> Serious concerns also arise when verifying whether a "parent or legal guardian," undefined in the bill, is in fact a minor's legal parent or guardian. Many parents and legal guardians do not share the same last name as their children due to remarriage, adoption, or other cultural or family-oriented decisions.

> If there is no authentication that a "parent" is actually a minor's legal parent or guardian, this may incentivize minors to ask other adults who are not their legal parent or guardian to verify their age on behalf of the minor to register for an account with a "large social media platform." It is also unclear who would be able to give consent to a minor in foster care or other nuanced familial situations, creating significant equity concerns.
> SB 1444 could also have broad impacts on other marginalized communities. For example, employing such tools could be abused by parents who overly restrict a child's access to information. LGBTQ+ youth could be subject to additional restrictions in connecting with like-minded individuals, particularly in households where their parents or guardians may not support or agree with their orientation. Similarly, a teen could be seeking reproductive health resources when they do not feel comfortable having such important and consequential conversations with their parents or guardians. Or, a child could be living in an abusive or otherwise unsafe household, and using additional measures to track and monitor that child could allow an abuser to exert additional control and harmful restrictions.

Oakland Privacy writes in an oppose unless amended position:

> [W]e think it is important to state that the challenge of maintaining positive relationships between parents and adolescents is not always as simple as a technology babysitter, and outsourcing parental attention to the trust level between them and their teenage children is not a fail-safe solution. In some cases, monitoring social media may make a bad situation worse, and cut off already alienated adolescents from outside sources of support, affirmation and mental health assistance. There is no "app" that will fix bad family dynamics.
>
> [Internet safety applications (ISA)] will obviously set their own parameters and criteria for what constitutes evidence of an adolescent's anxiety or depression. We can assume that some of these will be different from app to app and that parents will seek out ISA's that match their own opinions. It's not clear to us that such criteria will necessarily match clinical mental health indicators, accepted mental health parameters or even common sense. For example, is a teenager that is so upset about climate change that they want to engage in civil disobedience with the Sunrise Movement unduly "anxious"? What about a youth who wants to go vegan due to upset about factory farming?" Or who is interested in converting their religion to another one? Any of these beliefs or feelings may be deeply offensive to their parents, but are they "anxieties" that should be reported to their parents? Similarly, depression can be characterized in many ways. These are far too subjective indicators to be diagnosed accurately by a third party application, and they risk wildly

inappropriate and potentially destructive interventions by otherwise inattentive parents who have been alarmed by an "app" into confronting their children with cherry picked evidence pulled from their personal communications with their friends on social media.

5. Amendments

In response to the issues highlighted above, the author has engaged stakeholders to identify amendments to mitigate those concerns and has committed to continuing that process. The author has agreed to take the following amendments:

- Require third-party safety software providers to at least annually enlist a qualified independent auditing firm from a list to be created by the Attorney General to audit its privacy, security, and legal compliance. The audit shall be provided to the Attorney General, who shall review the audit, and include a summary of the audit findings on its publicly-accessible listing of third-party safety software providers. However, proprietary or confidential information shall not be disclosed to the public.
- Require user data to be deleted within 21 days of initial receipt.
- Conform the definition of social media platform to align with that in Business and Professions Code section 22675.

SUPPORT

Organization for Social Media Safety (sponsor)
Becca Schmill Foundation
Buckets Over Bullying
Childrens Advocacy Institute
D.A.R.E. America
Drug Induced Homicide
Mothers Against Prescription Drug Abuse (MAPDA)
Parent ProTech Inc.
Parents Television and Media Council
Protect Young Eyes
Sel4ca
8 individuals

OPPOSITION

California Chamber of Commerce
Chamber of Progress
Computer & Communications Industry Association
Electronic Frontier Foundation
Netchoice

Oakland Privacy
Technet

RELATED LEGISLATION

Pending Legislation:

SB 981 (Wahab, 2024) requires a social media platform to provide a mechanism that is reasonably accessible to users for a user who is a California resident to report nonconsensual, sexual deep fakes to the social media platform and to permanently block such content. SB 981 is currently in this Committee.

AB 3172 (Lowenthal, 2024) makes social media platforms liable for specified damages in addition to any other remedy provided by law, if the platform fails to exercise ordinary care or skill toward a child. AB 3172 is currently in the Assembly Judiciary Committee.

AB 3080 (Alanis, 2024) requires a covered platform, as defined, that publishes or distributes material harmful to minors, as defined, to perform reasonable age verification methods, as defined, to verify the age of each individual attempting to access the material and to prevent access by minors to the material. AB 3080 is currently in the Assembly Judiciary Committee.

Prior Legislation:

SB 287 (Skinner, 2023) would have subjected social media platforms to civil liability for damages caused by their designs, algorithms, or features, as provided. It would have provided a safe harbor where certain auditing practices are carried out. SB 287 was held in the Senate Appropriations Committee.

AB 1394 (Wicks, Ch. 579, Stats. 2023) required social media platforms to provide a reporting mechanism for suspected child sexual abuse material and requires them to permanently block the material, as provided. It also prohibits platforms from knowingly facilitating, aiding, or abetting minor's commercial sexual exploitation.

SB 1056 (Umberg, Ch. 881, Stats. 2022) required a social media platform, as defined, to clearly and conspicuously state whether it has a mechanism for reporting violent posts, as defined; and allows a person who is the target, or who believes they are the target, of a violent post to seek an injunction to have the violent post removed.

AB 587 (Gabriel, Ch. 269, Stats. 2022) required social media companies, as defined, to post their terms of service and report certain information to the Attorney General on a quarterly basis.

AB 1628 (Ramos, Ch. 432, Stats. 2022) required a social media platform, as defined, that operates in this state to create and publicly post a policy statement including specified information pertaining to the use of the platform to illegally distribute controlled substances, until January 1, 2028.

AB 2273 (Wicks, Ch. 320, Stats. 2022) established the California Age-Appropriate Design Code Act, placing a series of obligations and restriction on businesses that provide online services, products, or features likely to be accessed by a child.

AB 2408 (Cunningham, 2022) would have prohibited a social media platform from using a design, feature, or affordance that the platform knew, or which by the exercise of reasonable care it should have known, causes child users to become addicted to the platform. AB 2408 died in the Senate Appropriations Committee.

AB 2571 (Bauer-Kahan, Ch. 77, Stats. 2022) prohibited firearm industry members from advertising or marketing, as defined, firearm-related products to minors. This bill restricts the use of minors' personal information in connection with marketing or advertising firearm-related products to those minors.

AB 2879 (Low, Ch. 700, Stats. 2022) required a social media platform to disclose its cyberbullying reporting procedures in its terms of service and to have a mechanism for reporting cyberbullying that is available to individuals whether or not they have an account on the platform.

AB 1114 (Gallagher, 2021) would have required a social media company located in California to develop a policy or mechanism to address content or communications that constitute unprotected speech, including obscenity, incitement of imminent lawless action, and true threats, or that purport to state factual information that is demonstrably false. AB 1114 died in the Assembly Arts, Entertainment, Sports, Tourism, and Internet Media Committee.

SB 388 (Stern, 2021) would have required a social media platform company, as defined, that, in combination with each subsidiary and affiliate of the service, has 25,000,000 or more unique monthly visitors or users for a majority of the preceding 12 months, to report to the Department of Justice by April 1, 2022, and annually thereafter, certain information relating to its efforts to prevent, mitigate the effects of, and remove potentially harmful content. This bill died in the Senate Judiciary Committee.

****