SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

AB 2273 (Wicks)
Version: April 26, 2022
Hearing Date: June 28, 2022
Fiscal: Yes
Urgency: No
CK

SUBJECT

The California Age-Appropriate Design Code Act

DIGEST

This bill establishes the California Age-Appropriate Design Code Act, placing a series of obligations and restrictions on businesses that provide online services, products, or features likely to be accessed by a child. The bill tasks the California Privacy Protection Agency with establishing a taskforce to evaluate best practice and to adopt regulations.

EXECUTIVE SUMMARY

The General Data Protection Regulation (GDPR) is a regulation in European Union law on data protection and privacy. The law that implemented the GDPR in the United Kingdom included an amendment that effectuated the requirement to offer children-specific protections and required the Information Commissioner to introduce an Age Appropriate Design Code to set standards that make online services' use of children's data "age appropriate."

This bill, modeled after the Age Appropriate Design Code recently enacted in the United Kingdom, institutes a series of obligations and restrictions on businesses that provide an online service, product, or feature likely to be accessed by a child. The bill additionally requires the California Privacy Protection Agency (PPA) to establish a taskforce to evaluate best practices for the implementation of the bill's provisions, to provide support to businesses, and to adopt regulations, as necessary, by a certain date.

The bill is co-sponsored by the 5Rights Foundation and Common Sense. It is supported by a variety of groups, including Oakland Privacy. It is opposed by a variety of groups, including TechNet and the California Chamber of Commerce.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the federal Children's Online Privacy Protection Act (COPPA) to provide protections and regulations regarding the collection of personal information from children under the age of 13. (15 U.S.C. § 6501 et seq.)

2) Provides, in federal law, that a provider or user of an interactive computer service shall not be treated as the publisher or speaker of any information provided by another information content provider. (47 U.S.C. § 230(c)(2).)

3) Provides that a provider or user of an interactive computer service shall not be held liable on account of:
    a) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
    b) any action taken to enable or make available to information content providers or others the technical means to restrict access to such material. (47 U.S.C. § 230(c)(2).)

Existing state law:

1) 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).)

2) 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.)

3) 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.)

4) Establishes the California Consumer Privacy Act (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.)

This bill:

1) Requires a business that provides an online service, product, or feature likely to be accessed by a child ("covered business") to comply with all of the following:
    a) undertake a Data Protection Impact Assessment for any online service, product, or feature likely to be accessed by a child and maintain documentation of this assessment as long as the online service, product, or feature is likely to be accessed by a child;

b) provide a report of the assessment to the California Privacy Protection Agency ("agency") within the first year, with reviews every 24 months or before new features are offered to the public;
c) establish the age of consumers 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;
d) configure all default privacy settings offered by the online service, product, or feature to the settings that offer a high level of privacy protection offered by the business;
e) 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;
f) 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 their location, provide an obvious signal to the child when they are being monitored or tracked;
g) enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children; and
h) provide prominent, accessible, and responsive tools to help children, or where applicable their parent or guardian, exercise their privacy rights and report concerns.

2) Provides that a covered business shall not:
a) use the personal information of any child in a way that the business knows or has reason to know the online service, product, or feature more likely than not causes or contributes to a more than de minimis risk of harm to the physical health, mental health, or well-being of a child;
b) profile a child by default;
c) collect, sell, share, or retain any personal information that is not necessary to provide a service, product, or feature with which a child is actively and knowingly engaged;
d) if a business does not have actual knowledge of the age of a consumer, it shall not collect, share, sell, or retain any personal information that is not necessary to provide a service, product, or feature with which a consumer is actively and knowingly engaged;
e) use the personal information of a child for any reason other than the reason or reasons for which that personal information was collected. If the business does not have actual knowledge of the age of the consumer, the business shall not use any personal information for any reason other than the reason or reasons for which that personal information was collected;

f) notwithstanding Section 1798.120, share or sell the personal information of any child unless the sharing or selling of that personal information is necessary to provide the online service, product, or feature as permitted by paragraphs (1) to (4), inclusive, of subdivision (a) of Section 1798.145;
g) collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is 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;
h) collect, sell, or share 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;
i) use dark patterns or other techniques to lead or encourage consumers to provide personal information beyond what is reasonably expected for the service the child is accessing and necessary to provide that service or product to forego privacy protections, or to otherwise take any action that the business knows or has reason to know the online service or product more likely than not causes or contributes to a more than de minimis risk of harm to the child's physical health, mental health, or well-being; or
j) use any personal information collected or processed to establish age or age range for any other purpose, or retain that personal information longer than necessary to establish age. Age assurance shall be proportionate to the risks and data practice of a service, product, or feature.

3) Requires the PPA to establish and convene a taskforce, the California Children's Data Protection Taskforce, to evaluate best practices for the implementation of the bill, and to provide support to businesses, with an emphasis on small and medium businesses, to comply.

4) Requires the PPA's board to appoint, by April 1, 2023, members of the taskforce. Taskforce members shall consist of Californians with expertise in the areas of privacy, physical health, mental health and well-being, technology, and children's rights.

5) Requires the taskforce to make recommendations on best practices regarding, but not limited to, all of the following:
   a) identifying online services, products, or features likely to be accessed by children;
   b) evaluating and prioritizing the best interests of children with respect to their privacy, health, and well-being, and issuing guidance to businesses on how those interests may be furthered by the design, development, and implementation of an online service, product, or feature;
   c) ensuring that age verification methods used by businesses that provide online services, products, or features likely to be accessed by children are

proportionate to the risks that arise from the data management practices of the business, privacy protective, and minimally invasive;
d) assessing and mitigating risks to children that arise from the use of an online service, product, or feature, including specific issues businesses must address to perform a Data Protection Impact Assessment; and
e) publishing privacy information, policies, and standards in concise, clear language suited for the age of children likely to access that service or product.

6) Requires the PPA to adopt regulations, as necessary, in consultation with the taskforce, by April 1, 2024.

7) Codifies that the Legislature declares that children should be afforded protections not only by online products and services specifically directed at them, but by all online products and services they are likely to access and makes the following findings:
   a) companies that develop and provide online services, products, or features that children are likely to access should consider the best interests of children when designing, developing, and providing that service, product, or feature; and
   b) if a conflict arises between commercial interests and the best interests of children, companies should prioritizes the privacy, safety, and well-being of children over commercial interests.

8) Declares that it furthers the purposes and intent of the California Privacy Rights Act of 2020.

COMMENTS

1. Children online

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.

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."[1] A meta-analysis of research on social networking site (SNS) use concluded the studies supported an association between problematic SNS

[1] Zaheer Hussain and Mark D Griffiths, *Problematic Social Networking Site Use and Comorbid Psychiatric Disorders: A Systematic Review of Recent Large-Scale Studies*."

use and psychiatric disorder symptoms, particularly in adolescents.[2] The study found most associations were between such problematic use and depression and anxiety.

As pointed out by recent Wall Street Journal reporting, the companies' employees are aware of the dangers:

> A Facebook Inc. team had a blunt message for senior executives. The company's algorithms weren't bringing people together. They were driving people apart.
>
> "Our algorithms exploit the human brain's attraction to divisiveness," read a slide from a 2018 presentation. "If left unchecked," it warned, Facebook would feed users "more and more divisive content in an effort to gain user attention & increase time on the platform."
>
> That presentation went to the heart of a question dogging Facebook almost since its founding: Does its platform aggravate polarization and tribal behavior?
>
> The answer it found, in some cases, was yes.[3]

A recent New York Times article on leadership at Facebook elaborates:

> To achieve its record-setting growth, the [Facebook] had continued building on its core technology, making business decisions based on how many hours of the day people spent on Facebook and how many times a day they returned. Facebook's algorithms didn't measure if the magnetic force pulling them back to Facebook was the habit of wishing a friend happy birthday, or a rabbit hole of conspiracies and misinformation.
>
> Facebook's problems were features, not bugs.[4]

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

(December 14, 2018) Frontiers in psychiatry vol. 9 686, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6302102/pdf/fpsyt-09-00686.pdf. All internet citations are current as of June 23, 2022.

[2] *Ibid.*

[3] Jeff Horowitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive* (May 26, 2020) Wall Street Journal, https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

[4] Sheera Frenkel & Cecilia Kang, *Mark Zuckerberg and Sheryl Sandberg's Partnership Did Not Survive Trump* (July 8, 2021) The New York Times, https://www.nytimes.com/2021/07/08/business/mark-zuckerberg-sheryl-sandberg-facebook.html.

> 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.[5]

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:

> "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.

---

[5] 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.

> 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 . . . .[6]

The released documents from Instagram make clear that "Facebook is acutely aware that the products and systems central to its business success routinely fail":

> The features that Instagram identifies as most harmful to teens appear to be at the platform's core.
>
> The tendency to share only the best moments, a pressure to look perfect and an addictive product can send teens spiraling toward eating disorders, an unhealthy sense of their own bodies and depression, March 2020 internal research states. It warns that the Explore page, which serves users photos and videos curated by an algorithm, can send users deep into content that can be harmful.
>
> "Aspects of Instagram exacerbate each other to create a perfect storm," the research states.[7]

There are also growing concerns about the systematic collection of information from children and its utilization to target children with advertising or to ensure prolonged engagement with various media. While advertising to children and teenagers via various forms of media is not new, it has reached new heights. In 2018 in the United States, over $3 billion was spent on nondigital and $900 million for digital advertising on children.[8] Children and teenagers encounter advertising through an assortment of media and forms, including mobile apps and games that advertise specific brands. A 2020 policy statement published by the American Academy of Pediatrics explains the dangers of sophisticated utilization of children's personal information for targeted advertising or engagement:

> [M]ost research on children's understanding of advertising involves television and print ads only, but newer forms of advertising found in

---

[6] 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.
[7] *Ibid.*
[8] Jenny Redesky et al., *Digital Advertising to Children* (July 2020) AAP Council on Communication and Media, Pediatrics, Vol. 146, No. 1, https://publications.aap.org/pediatrics/article/146/1/e20201681/37013/Digital-Advertising-to-Children?autologincheck=redirected.

> mobile and interactive media and smart technologies, often powered by personal data, are more difficult to identify. They do not necessarily occur in a predictable manner and are often integrated into the content. Advertising may also be linked to rewards or be embedded in trusted social networks or personalized digital platforms, which may undermine children's abilities to identify or critically think about advertising messages. Regulations on television advertising have not yet been updated for the modern digital environment. . . .
>
> The nature of media used by children and teenagers has changed dramatically in the past decade, and children now spend more time on the Internet, social media, user-created content, video games, mobile applications (apps), virtual or augmented reality, virtual assistants, and Internet-connected toys. The Internet allows advertisers to contact, track, and influence users, as guided by behavioral data collection; a user's digital trail of location, activities, in-app behavior, likes, and dislikes contributes to a digital profile shared among many companies that can be used to make advertising messages more effective.[9]

The AAP statement elaborates on the depth and ubiquity of data collection and the vulnerability of children to its reach and consequences:

> Data collection for commercial purposes includes use of cookies in a user's browser, which record and follow Web page history; the collection of posts, likes, purchases, and viewing history by apps such as Facebook and Instagram or search engines such as Google; and collection of data via apps granted permission to track device data, such as location or contacts. Software mines such data from user accounts, devices, and virtual assistants and often shares data with third-party companies to develop a profile of the user, which informs the delivery of targeted ads. . . . User data can be aggregated and stored, sold to third parties, and used to infer personal characteristics, such as sexual orientation or health problems. . . .
>
> [S]tudies suggest that teenagers have a more interpersonal, and less technical, conceptualization of privacy, so they may not be as aware of the ramifications of sharing data with governments or corporations compared with sharing private information with friends or parents. Young children are more trusting of privacy-invasive technologies, such as location trackers, likely because of their convenience.

[9] *Ibid.*

2. Responding to these concerns abroad

As stated, the UK has recently implemented the Age Appropriate Design Code to set standards that make online services' use of children's data "age appropriate": "The Children's code (or the Age appropriate design code) contains 15 standards that online services need to follow. This ensures they are complying with [their] obligations under data protection law to protect children's data online."

The UK Information Commissioner provides detail on implementation and vision:

> Data sits at the heart of the digital services children use every day. From the moment a young person opens an app, plays a game or loads a website, data begins to be gathered. Who's using the service? How are they using it? How frequently? Where from? On what device?
>
> That information may then inform techniques used to persuade young people to spend more time using services, to shape the content they are encouraged to engage with, and to tailor the advertisements they see.
>
> For all the benefits the digital economy can offer children, we are not currently creating a safe space for them to learn, explore and play.
>
> This statutory code of practice looks to change that, not by seeking to protect children from the digital world, but by protecting them within it.
>
> **This code is necessary.**
>
> This code will lead to changes that will help empower both adults and children.
>
> One in five UK internet users are children, but they are using an internet that was not designed for them.

3. Existing laws protecting children's privacy

The Children's Online Privacy Protection Act of 1998 (COPPA) imposes requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. (15 U.S.C.S. § 6501; 16 C.F.R. Part 312.) COPPA makes it unlawful for any operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Broadly, COPPA requires these operators to do the following:

- provide notice on the Web site or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information;
- obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children;
- provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance;
- not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
- establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

The Student Online Personal Information Protection Act (SOPIPA) restricts the use and disclosure of the personally identifiable information or materials of K-12 students. (Bus. & Prof. Code § 22584.) It regulates operators of Internet Web sites, online services, online applications, or mobile applications with actual knowledge that the sites, services, or applications are used primarily for K–12 school purposes and were designed and marketed for K–12 school purposes. It prohibits operators from knowingly engaging in specified activities with respect to their site, service, or application. This includes:

- engaging in targeted advertising when the targeting of the advertising is based upon any information that the operator has acquired because of the use of that operator's site, service, or application;
- use of information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile about a K–12 student except in furtherance of K–12 school purposes; or
- selling a student's information.

SOPIPA also restricts disclosing the information but provides various exceptions, including where the disclosure is in furtherance of the K–12 purpose of the site, service, or application. Operators are also required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and protect that information from unauthorized access, destruction, use, modification, or disclosure. They must delete a student's information if the school or district requests deletion of data under the control of the school or district.

The CCPA 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. (Civ. Code § 1798.100 et seq.) It places attendant obligations on businesses to respect those rights. In the November 3, 2020 election, voters approved Proposition 24, which established the CPRA. The CPRA amends the CCPA, limits further amendment, and creates the PPA.

The CPRA 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.)

4. Establishing the California Age-Appropriate Design Code Act.

President Biden has emphasized the critical need for a response to the issues discussed above: "We must hold social media platforms accountable for the national experiment they're conducting on our children. It's time to strengthen privacy protections, ban targeted advertising to children, and demand tech companies stop collecting personal data on our children."

This bill, modeled after the Age Appropriate Design Code enacted in the United Kingdom, responds to this call to action. It institutes a series of obligations and restrictions on businesses that provide an online service, product, or feature likely to be accessed by a child ("covered business"). That term, "likely to be accessed by a child," means it is reasonable to expect, based on the nature of the content, the associated marketing, the online context, or academic or internal research, that the service, product, or feature would be accessed by children. The bill requires these covered businesses to approach design, data collection, and their offerings to better serve the best interests of children.

a. Requiring someone to think about the children: child-centered design and approaches

Businesses that provide an online service, product, or feature likely to be accessed by a child are required to make privacy protections for children the default by configuring all default privacy settings offered by the online service, product, or feature to the settings that offer a high level of privacy protection offered by the business. They are prohibited from profiling children by default. Covered businesses are required to provide privacy information, terms of service, policies, and community standards in a manner that is accessible to children likely to access it and to enforce those policies and standards.

Covered businesses must establish the age of consumers 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.

Covered businesses are also required to undertake "Data Protection Impact Assessments" for any online service, product, or feature likely to be accessed by a child, maintain documentation of this assessment, and provide a report to the PPA within a year of implementation of this bill.

A data protection impact assessment is defined as a systematic survey to assess and mitigate risks to children who are reasonably likely to access the service, product, or feature at issue that arises from the provision of that service, product, or feature in accordance with specifications promulgated by the California Children's Data Protection Taskforce, discussed below. The assessments must be reviewed every 24 months or before any new features are offered to the public.

b. Curtailing problematic data collection practices

Businesses that provide an online service, product, or feature likely to be accessed by a child are also prohibited from a number of data collection and use practices with regard to children and the services and products they access.

A covered business cannot collect, sell, share, or retain any personal information that is not necessary to provide a service, product, or feature unless the business has actual knowledge the consumer is not a child. Additionally, if it is precise geolocation information, it can only be for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature. Such sensitive location information can only be collected when providing an obvious sign to the child that such collection is happening for the duration of the collection.

These provisions provide a strong protection for users, making the default data collection abide by data minimization principles. Only when it is determined that a user is not a child can personal information be collected, sold, shared, or retained beyond what is necessary for the user's interaction with the business' service, product, or feature.

Based on this same principle, the bill also does not allow a covered business to use personal information for any reason other than the reason or reasons for which that personal information was collected unless the business has actual knowledge the consumer is not a child.

These businesses are also prohibited from using the personal information of any child in a way that the business knows or has reason to know the online service, product, or feature more likely than not causes or contributes to a more than de minimis risk of harm to the physical health, mental health, or well-being of a child. This centers children's health and welfare over other priorities. Where such risk of harm exists, businesses are able to continue to use the information for purposes other than what it was collected for once they have confirmed the user is not a child.

The bill also looks to protect problematic tactics to deepen the data collection. Specifically, these businesses cannot use dark patterns or other techniques to lead or encourage consumers:

- to provide personal information beyond what is reasonably expected for the service the child is accessing and necessary to provide that service or product;
- to forego privacy protections; or
- to otherwise take any action that the business knows or has reason to know the online service or product more likely than not causes or contributes to a more than de minimis risk of harm to the child's physical health, mental health, or well-being.

The section of the bill laying out these restrictions on businesses' data collection practices when children are involved includes some slightly duplicative provisions and some sections that could benefit from more clarity. In response, the author has agreed to the following amendments that address these concerns and streamline the bill:

Amendment

Amend Section 1798.99.31(b) as follows:

(b) A business that provides an online service, product, or feature likely to be accessed by a child shall not take any of the following actions:
(1) Use the personal information of any child in a way that the business knows or has reason to know the online service, product, or feature more likely than not causes or contributes to a more than de minimis risk of harm to the physical health, mental health, or well-being of a child.
(2) Profile a child by default.
(3) Collect, sell, share, or retain any personal information that is not necessary to provide a service, product, or feature with which a child is actively and knowingly engaged**, or as described in paragraphs (1) to (4), inclusive, of subdivision (a) of Section 1798.145.**
(4) Use personal information for any reason other than the reason or reasons for which that personal information was collected, where the end user is a child.
~~**(4) If a business does not have actual knowledge of the age of a consumer, it shall not collect, share, sell, or retain any personal information that is not necessary to provide a service, product, or feature with which a consumer is actively and knowingly engaged.**~~
~~**(5) Use the personal information of a child for any reason other than the reason or reasons for which that personal information was collected. If the business does not have actual knowledge of the age of the consumer, the business shall not use any personal information for any reason other than the reason or reasons for which that personal information was collected.**~~

~~**(6) Notwithstanding Section 1798.120, share or sell the personal information of any child unless the sharing or selling of that personal information is necessary to provide the online service, product, or feature as permitted by paragraphs (1) to (4), inclusive, of subdivision (a) of Section 1798.145.**~~
(7) Collect, sell, or share any precise geolocation information of children by default unless the collection of that precise geolocation information is necessary **for the business** 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.
(8) Collect~~**, sell, or share**~~ any precise geolocation information **of a child** without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected.
(9) Use dark patterns ~~**or other techniques**~~ to lead or encourage ~~**consumers**~~ **children** to provide personal information beyond what is reasonably expected ~~**for the service the child is accessing and necessary**~~ to provide that **online service, product or feature,** ~~**or product**~~ to forego privacy protections, or to ~~**otherwise**~~ take any action that the business knows or has reason to know ~~**the online service, or product,**~~ more likely than not causes or contributes to a more than de minimis risk of harm to the child's physical health, mental health, or well-being.
(10) Use any personal information collected or processed to establish age or age range for any other purpose, or retain that personal information longer than necessary to establish age. Age assurance shall be proportionate to the risks and data practice of a service, product, or feature.

c. Establishing a taskforce and developing regulations

The bill additionally requires the PPA to establish a taskforce and appoint its members, who should be experts in specified fields, including privacy and technology. The taskforce will be called the California Children's Data Protection Taskforce and will evaluate best practices for the implementation of the bill's provisions, and provide support to businesses. The PPA, in consultation with the task force, is required to adopt regulations, as necessary, by April 1, 2024. Concerns have been raised about how the taskforce will be constituted and the clarity of their mission. The author may wish to consider further refinement to ensure maximal effectiveness.

5. Stakeholder positions

According to the author:

> The Internet is increasingly shaping how children socialize, consume entertainment, create, and learn. According to data from UNICEF, approximately one in three internet users is a child under 18 years of age. Among parents with children who have access to the internet, there is a

> concern about what kids are accessing, and the potential harmful effects of the way that access occurs. Data from Parents Together show that 85 percent of parents are concerned with how much time their kids are spending online – time that has increased since the pandemic. The same percentage of parents think that Congress should require protections for kids online, and help to stop sexual predators, place limits on deceptive advertising and protect children's privacy.
>
> Data privacy for children is especially important because its misuse can expose children to harmful material, compulsive behavior loops, and other risks. For example, research from the 5Rights Foundation found that, of the top 100 free apps for kids in one of the major app stores, one in three have overt banner ads, including ads that promote adult-appropriate apps requiring a user to watch the full promo before a box could be closed. Additionally, only 36 percent of California teens and 32 percent of California parents say that social networks do a good job explaining what they do with users' data.
>
> While existing federal and state privacy laws offer important protections that guard children's privacy, there is no coherent, comprehensive law that protects children under 18 from goods, services, and products that endanger their welfare. As a result, online goods, services, and products that are likely to be accessed by kids have been loaded with adult design principals that do not factor in the unique needs of young minds, abilities, and sensibilities, nor offer the highest privacy protections by design and by default. As a result, children under 18 face a number of adverse impacts due to their interactions with online world, including bullying, mental health challenges, and addictive behaviors.

An opposition coalition, including the Entertainment Software Association, argues that the "likely to be accessed by a child" standard is too broad and has requested replacing it with the "directed at children" standard found in COPPA:

> In order to ensure our companies are able to implement this bill effectively we suggest aligning the scope of AB 2273 with existing law and definitions, namely by changing "likely to be accessed by a child" to "directed to children". "Likely to be accessed by a child" is an overinclusive standard and would capture far more websites and platforms than necessary and subject them to this bill's requirements. It is also an unfamiliar standard that will present problems for companies trying to determine whether they are in the scope of the bill.
>
> "Directed to children" on the other hand is a term and scope that online services are familiar with as it is defined in COPPA, which companies

> have been implementing and complying with since its passage over 20 years ago. Similarly, we suggest aligning the definition of "child" with COPPA as a person under the age of 13.

However, the "directed at" standard is extremely narrow and would carve out most of the places children are actually found online. The author disagrees that the standard should be "directed at": "The Code is designed to ensure companies children are using design their products in an age-appropriate manner with the best interest of children. This is about meeting children where they are online, not making Sesame Street safer for children." In addition, the workability of the standard is holding up in the United Kingdom where this has been the law. However, to address concerns that the likely to be accessed" standard does not provide enough clarity, the author has agreed to the following amendment that outlines the criteria:

> Amendment
>
> (6) "Likely to be accessed by a child" means it is reasonable to expect, based on the ~~**nature of the content, the associated marketing, the online context, or academic or internal research, that the service, product, or feature would be accessed by children.**~~ **following factors that the online service, product, or feature would be accessed by children:**
>
> **A. The online product, service, or feature is directed at children as defined by COPPA.**
>
> **B. The online product, service, or feature is determined to be routinely accessed by children through academic, market, or internal company research.**
>
> **C. An online product, service, or feature advertises to children.**
>
> **D. An online product, service, or feature that is substantially similar or the same as an online service, product, or feature covered by paragraph (B).**
>
> **E. An online product, service or feature that has design elements that are known to be of interest to children, including but not limited to, games, cartoons, music, and celebrities who appeal to children.**

This language cabins which online services, products, and features are subject to the bill's obligations and restrictions. It tailors the definition to a narrower range of businesses while still effectuating the strong policy objectives.

Privacy concerns have been raised that the age verification requirements of the bill are going to result in more invasive data collection practices. It should be noted that these businesses are prohibited from using any personal information collected or processed to establish age or age range for any other purpose or retain it longer than necessary to

establish age. The bill also tries to more precisely calibrate the intensity of the required data collection for age verification to the risks and data practice of a service, product, or feature, but a number of provisions will lead to many businesses automatically age-gating their services.

Tim Kendall, the first Director of Monetization at Facebook, "created the advertising model that has driven the company's massive profitability and growth." He writes in support:

> I know from experience that tech workers want to innovate and design products differently to prioritize well-being over profit. But until the profit motive changes, design will be at the expense of our collective well-being, especially our kids'. To change the incentives, we need our political leaders to act. And we need solutions that work.
>
> The world's largest tech companies have already said that the Age Appropriate Design Code, law in the United Kingdom, is spurring positive change. Just last month, a senior Google official told the UK Parliament, "The Age Appropriate Design Code has helped us determine new ways to keep our users safe."
>
> Wouldn't they want to ensure California kids, kids in the United States, are safe as well? By taking some very basic steps – like restricting the collection of kids' data, requiring high privacy settings by default, and providing young people clear resources to report abusive users or block unpleasant content – the State of California can protect the health and wellbeing of millions of young people in our state.
>
> We need lawmakers to regulate in order to shift the incentive structure of the tech industry. Historically, the regulation and enforcement of laws has been a primary catalyst in spurring innovation in virtually every new technology this country has seen. There is no doubt that regulating safer children's experiences online will lead to all kinds of technological innovation.
>
> The California Age Appropriate Design Code Act – already in practice in the UK – gives us the opportunity to usher in a new era of innovative product design that considers, rather than monetizes, the next generation.

Writing in support, Roblox argues:

> The United Kingdom's Age-Appropriate Design Code (AADC) came into effect in September 2021. Despite the fact that it is a Code of Practice specific to the UK, Roblox chose to introduce many of its protections

> globally. We believe that when safety practices faithfully serve the needs of all young people, it makes sense to apply them universally. Consistent with this philosophy, we welcome the introduction of AB 2273 in California, formalizing such protections for California's youth.
>
> Specifically, we note the following characteristics of AB 2273:
>
> - It is Principle-Based: Principle-based approaches to safety promote accountability while remaining flexible enough to allow for future innovation and changes in the technology landscape. Further, as a principles-based approach, the Code can be applied to the diversity of services that are offered to children online today, from nascent, start-up technologies to large, global platforms.
> - It is Risk-Based: Companies are often best positioned to address vulnerabilities that may exist on their platforms. The risk-based approach that underpins AB 2273 allows for a service-specific means to managing potential risks, avoiding the unintended consequences that a "one size fits all" approach can bring to privacy and safety.
> - It Emphasizes the "Best Interests of the Child": AB 2273 requires companies to consider the "best interests of the child" in designing and creating tools and features, helping to ensure that children's well-being remains a key part of the design and implementation process.
> - It is Modeled After Existing Legislation: Having seen similar measures to AB 2273 thoughtfully introduced and implemented by UK policymakers last year, we believe they can scale effectively for children in California.

The opposition coalition also argues for a narrow enforcement mechanism:

> We also suggest enumerating a clear enforcement mechanism such as the one found in CCPA, which grants the Attorney General the authority to investigate and enforce violations. We believe the Attorney General is the appropriate agency to enforce this bill provided our companies have the ability to seek guidance on this bill's subjective requirements and fix mistakes before fines or penalties are levied. The Attorney General's office is best equipped to provide consistent interpretations, guidance, and to enforce this bill's provisions.

In response, the author has agreed to amendments that grant authority to the Attorney General to enforce the bill's provisions and that explicitly preclude the bill serving as the basis for a private right of action:

Amendment:

Add: Sec. 1798.99.35 (a) Any business that violates this title shall be subject to an injunction and liable for a civil penalty of not more than $2,500 per affected child for each negligent violation or not more $7,500 per affected child for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(b) Nothing in this Title shall be interpreted to serve as the basis for a private right of action under this title.

SUPPORT

5Rights Foundation (co-sponsor)
Common Sense (co-sponsor)
Alcohol Justice
Accountable Tech
ADL West
Avaaz
California Lawyers Association, Privacy Law Section
Center for Countering Digital Hate
Center for Digital Democracy
Center for Humane Technology
Children and Screens
Consumer Federation of America
Consumer Federation of California
Do Curious INC.
Eating Disorders Coalition
Epic
Fair Vote
Fairplay
Je Suis Lá
Joan Ganz Cooney Center - Sesame Workshop
LiveMore ScreenLess
Log Off
Lookup
Me2b Alliance
National Hispanic Media Coalition
Neda
Oakland Privacy
Omidyar Network
Outschool, Inc.
Parents Together Action

Protect Young Eyes
Public Health Advocates
Real Facebook Oversight Board
Remind
Reset Tech
Roblox Corporation
Smart Digital Kids
Sum of Us
Tech Oversight Project
The Children's Partnership
The Signals Network
The Social Dilemma
Tiramisu
Ultraviolet
Two individuals

OPPOSITION

California Chamber of Commerce
Entertainment Software Association
MPA - the Association of Magazine Media
TechNet

RELATED LEGISLATION

Pending Legislation:

SB 1056 (Umberg, 2022) requires 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. This bill is currently in the Assembly Judiciary Committee.

AB 587 (Gabriel, 2022) requires social media companies, as defined, to post their terms of service and report certain information to the Attorney General on a quarterly basis. This bill is currently pending before this Committee and is being heard the same day as this bill.

AB 1628 (Ramos, 2022) requires online platforms to create and post a policy that includes policies regarding distribution of controlled substances and its prevention, reporting mechanisms, and resources. This bill is currently pending before this Committee and is being heard the same day as this bill.

AB 2408 (Cunningham, 2022) establishes a negligence cause of action for a platform's use of any design, feature, or affordance that causes a child user to become addicted to the platform. It also provides for heightened civil penalties in actions brought by public prosecutors. This bill is currently pending before this Committee and is being heard the same day as this bill.

AB 2571 (Bauer-Kahan, 2022) prohibits firearm industry members from advertising or marketing, as defined, firearm-related products to minors. The bill restricts the use of minors' personal information in connection with marketing or advertising firearm-related products to those minors. This bill is currently in the Senate Appropriations Committee.

AB 2879 (Low, 2022) requires social media platforms to implement a mechanism by which school administrators can report instances of cyberbullying, and to disclose specified data related to reported instances of cyberbullying and the platform's response. This bill is currently pending before this Committee and is being heard the same day as this bill.

Prior Legislation: None known.

PRIOR VOTES:

Assembly Floor (Ayes 72, Noes 0)
Assembly Appropriations Committee (Ayes 16, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)

****