Date of Hearing: April 22, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1043 (Wicks) – As Amended March 28, 2025

SUBJECT: Age verification signals: software applications and online services

SYNOPSIS

Over the last decade, the Legislature has worked to protect children from the potential harms they face on the largely unregulated internet. It would be unthinkable to most parents to leave their children alone in a public place to fend for themselves. However, when children spend time on the internet, they are often left unsupervised. The risks are significant. On platforms designed to optimize engagement, children can be subjected to cyberbullying, scammed, exposed to violent pornography, groomed in chat rooms, fed algorithmically-driven inappropriate content, and may develop unhealthy relationships with strangers and AI companions.

This bill, sponsored by the International Centre for Missing and Exploited Children and Children Now, seeks to require device and operating systems manufacturers to develop an age assurance signal that will be sent to application developers informing them of the age-bracket of the user who is downloading their application or entering their website. Depending on the age range of the user, a parent or guardian will have to consent prior to the user being allowed access to the platform. The bill presents a potentially elegant solution to a vexing problem underpinning many efforts to protect children online. However, there are several details to be worked out on the bill to ensure technical feasibility and that it strikes the appropriate balance between parental control and the autonomy of children, particularly older teens.

The bill is supported by several parents' organizations, including Parents for School Options, Protect our Kids, and Parents Support for Online Learning. In addition, the TransLatin Coalition and The Source LGBT+ Center are in support. The bill is opposed by Oakland Privacy, TechNet, and Chamber of Progress.

If passed by this Committee, the bill will next be heard by the Judiciary Committee.

THIS BILL:

1) Requires a manufacturer of a device or an operating system do all of the following:

    a) Provide an accessible interface that requires device owners to indicate the birth date, age, or both, of the user of the particular device.

        i) Limits the use of the data to providing a signal regarding the device user's age to all applications available in a covered application store.

    b) If the manufacturer is also an application store:

        i) Obtain parent or guardian consent before permitting a child under 16 to download an application.

ii) Provide a signal in the application store indicating whether a parent or guardian has provided consent.

iii) Provide an option to connect a parent with the application developer for the purpose of managing any parental control tools.

c) Provide application developers with a digital signal signaling whether or not a user is in any of the age brackets.

2) Requires an application developer that has actual knowledge that a user is under 18 via a signal regarding the users age, to the extent technically feasible, provide readily available features for parents to support a child users use of the application.

3) Requires an application developer to provide parents features that do all of the following, as appropriate given the risks that arise from the use of the application:

a) Help manage which accounts are linked to the child user.

b) Manage the delivery of age appropriate content.

c) Limit the amount of time that the child user spends daily on an application.

4) States that a signal is presumed to be accurate and that a developer may rely on the signal for the purpose of compliance with any state law that requires age verification or parental consent.

5) Defines the following:

a) "Age bracket data" means nonpersonally identifiable data derived from a user's birth date or age that indicates only the following:

i) Whether a user is under five years old.

ii) Whether a user is at least five, but under 10 years old.

iii) Whether a user is at least 10, but under 13 years old.

iv) Whether a user is at least 13, but under 16 years old.

v) Whether a user is at least 16, but under 18 years old.

vi) Whether a user is at least 18 years old.

b) "Application" means a software application or online service, product, or feature that may be run or directed by a user on a computer, mobile device, or any other general purpose computing device.

c) "Child" means a person who is under 18 years old.

d) "Covered application store" means a publicly available website, software application, online service or platform that allows a user to download an application from third-party developers.

e) "Covered manufacturer" means a person who is a manufacturer of a device, an operating system for a device, or a covered application store.

f) "Developer" means a person that creates, owns, or controls an application and is responsible for the design, development, maintenance, and distribution of the application.

g) "Online service, product, or feature" does not mean any of the following:

   i) A broadband internet access service.

   ii) A telecommunications service.

   iii) The delivery or use of a physical product.

h) "Signal" means age bracket data or notice of parental consent sent by a real-time secure application programming interface or operating system to an application.

i) Establishes that a person who violates this title shall be subject to an injunction and liable for a civil penalty of not more than $2,500 per child for a negligent violation or not more than $7,500 per child for an intentional violation.

j) The penalty will be assessed and recovered by a civil action brought by the Attorney General.

k) States that this title does not modify, impair, or supersede the operation of any antitrust law.

l) States that the protections provided by this title are in addition to those provided by any other applicable law, including the California Age-Appropriate Design Code Act.

EXISTING LAW:

1) States that Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. (U.S. Const., amend. I)

2) 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.)

3) Prohibits, under Section 230 of the Communications Decency Act, treating a provider or user of an interactive computer service as the publisher or speaker of any information provided by another information content provider. (47 U.S.C. § 230(c)(1).)

4) 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.)

5) Under the Protecting Our Kids from Social Media Addiction Act, prohibits an operator of an addictive internet-based service or application, including a social media platform, from providing an addictive feed, as defined, to a minor user, except as prescribed. (Health & Saf. Code § 27000 et seq.)

COMMENTS:

1) **Author's statement**. According to the author:

> California's children are growing up with access to an online world that was not built with them in mind. Kids rely on the digital world for education, entertainment, and socialization, but there are no guardrails that protect them from exposure to manipulative design features, and inappropriate interactions. This leaves children vulnerable to harm, including cyberbullying, sextortion, mental health struggles and more. This is simply unacceptable. It is essential that online spaces are designed with children's safety in mind from the outset — and a key part of that design is the ability to accurately assess a user's age.
>
> The Digital Age Assurance Act is a crucial step in ensuring kids can explore the digital world more safely — and a critical step needed for us to require social media and other online companies to implement higher consumer safety standards for products accessed by kids. The urgency behind AB 1043 is backed by mounting evidence of the harmful impacts unregulated digital environments can have on children's mental health, safety, and overall well-being. Creating a statutory age assurance framework that balances privacy and usability will give parents greater peace of mind, build trust with children and families, and create consistency for businesses looking to innovate responsibly. AB 1043 provides a scalable path forward — one that encourages the development of safer online experiences while preserving the benefits of digital participation for young users.

2) **Age verification.** Policymakers around the world have struggled in recent years to determine the best method for verifying the ages of internet users without eroding people's fundamental privacy rights. Among the most common ways of verifying age are requiring users to upload their government issued identification to prove their age or by allowing users to self-attest to their age.

Last year alone, this committee heard several bills related to protecting children's personal information, activities online, and attempting to tackle questions related to age verification. Among them:

- AB 1949 (Wicks), sponsored by Attorney General Rob Bonta, would have amended the California Consumer Privacy Act (CCPA) to prohibit businesses from collecting the personal information of a consumer under 18 years of age unless the consumer, or the consumer's parent or guardian if under 13, affirmatively authorizes the collection. That bill was vetoed by the Governor.

- AB 3080 (Alanis and Hoover) would have required online businesses that provide products that are illegal for children to access, take reasonable steps to ensure the user is of legal age

at the time of access, including, but not limited to, verifying the age of the user. Of particular concern for these authors was children's access to online pornography. That bill was held on the Senate Appropriations Committee's suspense file.

- SB 976 (Skinner; Stats. 2024, Ch. 321) established the Protecting our Kids from Social Media Addiction Act. The act prohibits social media companies from providing minors, without parental consent, addictive feeds, and from sending minors notifications during certain timeframes.

In commenting on last year's AB 3080 (Alanis), the Age Verification Providers Association, wrote about "the ease of use of the wide variety of methods of age verification, and the data minimization designed into these approaches so personally identifiable data need never be retained." They stated that "reasonable age verification methods" include:

> **Remote electronic identification verification technology (eIDVT**) – government issued physical identity documents such as passports or driving licenses are scanned as an image using the user's mobile phone camera or webcam, or, in some cases where this is included, a computer chip in the document can be read by a smartphone. The user is asked to provide a live selfie image which can then be electronically compared to the image from the ID, and provided the two match, then the age information is recorded and can then be used as the basis of age verification.
>
> […]
>
> **Online banking integration** – Some AV providers have reached agreement with banks to allow a customer to log into their online banking and give consent for the bank to confirm their date of birth to the AV provider.
>
> **Credit Reports and other transactional databases** – A user can give consent for an AV provider to check with Credit Report bureau if the age they are claiming is accurate. Typically, the user will have to give some further reassurance that they are the person whose credit report they are claiming belongs to them; for example, knowing about some recent payments they have made. Other authoritative databases can play a similar role, with their own approaches to authentication of the user claiming the age data relates to them.
>
> **Facial age estimation** – through machine learning, algorithms can now predict to within 1 ½ years mean average error the age of a user from a selfie image. The National Institute of Standards and Technology (NIST) have been testing competing solutions from providers and are expected to publish their findings this week, prior to the Committee's hearing. While some people have expressed concerns about adults sharing a selfie image for this purposes, it should be noted that the estimation can be made locally on the user's own phone or PC, so the image need never be shared with a third party. Given there is a margin for error, typically this would be made available as an option for users who are several years over 18 – for example, 23 – when it is statistically proven that the vast majority of minors under 18 would not be estimated to look at least 23. Users who are closer to 18 will need to use an alternative mechanism.
>
> […]

> **Reusable digital identity** – Digital ID is becoming increasingly available. Several US states issue mobile drivers licenses, for example. Users can give consent for the age to be selectively shared with AV providers, typically using an approach called Verifiable Credentials.

Commenting on the same earlier bill, the Free Speech Coalition, which advocates for the adult film industry, suggested in content-filters installed on personal computers:

> Filters are already available on phones, tablets, laptops and home WiFi networks. They are easy to set up and, for the most part, free to use. . . .
>
> Filters [cannot] be evaded by use of VPN — the virtual private networks that allow users to evade the regulations by accessing the internet through another state or country. Filters can be tailored to remove sites like Twitter and Reddit which allow adult content. . . . Filters can also trigger "safe search" settings on search engines, which prevent adult content or sites from appearing in search results.

A 2022 report by France's National Commission on Informatics and Liberty (CNIL) "analysed the main types of age verification systems in order to clarify its position on age verification on the Internet, particularly on pornographic sites for which such verification is mandatory. It specifies how such publishers could fulfil their legal obligations. However, CNIL finds that such current systems are circumventable and intrusive, and calls for the implementation of more privacy-friendly models."[1] A *Verge* article describing this report states: "CNIL notes that identifying someone's age with a credit card would be relatively easy since the security infrastructure is already there for online payments. But some adult users — especially those with lower incomes — may not have a card, which would seriously limit their ability to access online services. The same goes for verification methods using government-issued IDs. Children can also snap up a card that's lying around the house to verify their age." [2]

3) **Potentially harmful experiences on the internet.** The early 2010s saw a major upsurge in adolescent depression and anxiety, self-harm, and suicide. The trend is concentrated in Gen Z, and girls are more impacted than boys.[3] As of 2021, relative rates of depression teen girls and boys had increased by roughly 150% compared to 2010.[4] The trend is reflected in objective measures, including hospitalizations from self-harm. In 2020, young teenage girls were hospitalized for self-harm, primarily from cutting, at three times the rate they were in 2010.[5] Young teen suicide more than doubled in this timeframe.[6] Similar trends have been observed in several western countries.[7] These trends track "the years when adolescents in rich countries

---

[1] *Online age verification: balancing privacy and the protection of minors* (Sept 22, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.
[2] Roth, *Online age verification is coming, and privacy is on the chopping block* (May 15, 2023) The Verge, https://www.theverge.com/23721306/online-age-verification-privacy-laws-child-safety.
[3] Haidt, "The Teen Mental Illness Began Around 2012" *After Babel* (2023), https://www.afterbabel.com/p/the-teen-mental-illness-epidemic, summarizing Haidt et al, "Adolescent mood disorders since 2010: A collaborative review" (ongoing) available at https://docs.google.com/document/d/1diMysMeRphUH7E6D1d_J7R6WbDdgnzFHDHPx9HXzR5o/edit?tab=t.0#.
[4] "The Teen Mental Illness Began Around 2012," *supra*.
[5] *Id.* For older teens, the increase for girls was 48%; for boys, 37%.
[6] *Id.* For older teens, the increase for girls was 63.9%; for boys, 35%.
[7] A series of articles from Haidt and Rausch addresses this issue under the header "The International Mental Health Crisis" on Haidt's Substack, *After Babel*, https://www.afterbabel.com/t/the-international-mental-health-crisis.

traded their flip phones for smartphones and moved much more of their social lives online . . ."[8] Some specific types of harmful online experiences follow:

Social media. In May 2023, former Surgeon General Vivek Murthy issued an advisory warning of the potential mental health impacts of social media on young people. The advisory recognizes the benefits of social media for some users but concludes "the current body of evidence indicates that while social media may have benefits for some children and adolescents, there are ample indicators that social media can also have a profound risk of harm to the mental health and well-being of children and adolescents."[9] While noting that several complex factors shape social media's influence on children and adolescents, the Surgeon General points to two primary risk factors: 1) harmful content, and 2) excessive and problematic use. Harmful content includes:

- Extreme content such as live depictions of self-harm acts, like asphyxiation or cutting, "which can normalize such behaviors, including through the formation of suicide pacts and posing of self-harm models for others to follow."[10]

- Bullying and harassment: roughly two-thirds of adolescents are "often" or "sometimes" exposed to hate-based content, with nearly 75% adolescents stating that social media sites do a fair to poor job of addressing online harassment and bullying.[11]

- Predatory behaviors, including financial or sexual exploitation of children and adolescents; nearly 6-in-10 adolescent girls surveyed had received unwanted advances from strangers on social media platforms.[12]

The advisory also cites studies showing that on a typical weekday, nearly one in three adolescents report using screens – most commonly, social media – until midnight or later.[13] One third or more of girls aged 11-15 feel "addicted" to certain platforms. Excessive use correlates with attention problems, feelings of exclusion, and sleep problems.[14] Poor sleep, in turn, is linked with neurological development issues, depression, and suicidality.[15] These findings are borne out by the observations of platforms themselves: internal Meta research detailed in a recent lawsuit concluded that "when social media use displaces sleep in adolescents, it is negatively correlated

---

[8] Haidt, "End the Phone-Based Childhood Now" *The Atlantic* (March 13, 2024), https://www.theatlantic.com/technology/archive/2024/03/teen-childhood-smartphone-use-mental-health-effects/677722/.
[9] "Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory" (May 23, 2023) p. 4, https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf. ("Surgeon General's Advisory")
[10] *Ibid.*
[11] Alhajji et al., "Cyberbullying, Mental Health, and Violence in Adolescents and Associations With Sex and Race: Data From the 2015 Youth Risk Behavior Survey" *Global pediatric health* (2019), https://journals.sagepub.com/doi/10.1177/2333794X19868887; Vogels, "Teens and Cyberbullying," Pew Research Center*: Internet, Science & Tech* (2022), https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.
[12] Nesi, et al., "Teens and mental health: How girls really feel about social media" Common Sense Media (2023), https://www.commonsensemedia.org/research/teens-and-mental-health-how-girls-really-feel-about-social-media.
[13] Rideout, V., & Robb, M. B. "Social media, social life: Teens reveal their experiences" Common Sense Media (2018), https://www.commonsensemedia.org/sites/default/files/research/report/2018-social-mediasocial-life-executive-summary-web.pdf.
[14] Surgeon General's Advisory, *supra*, at p. 10.
[15] *Ibid.*

to indicators of mental health."[16] As of 2024, the average daily social media usage for US adolescents was 4.8 hours.[17]

Children's exposure to violent pornography. The widespread availability of violent pornography has reshaped the sexual expectations of young men and women, often in ways that are harmful to intimacy, consent, and mutual pleasure. Among the impacts are:

- Young men report that in consuming pornography they become desensitized and require more intense material to achieve the same level of arousal. This can result in young men developing unrealistic and aggressive sexual expectations that do not align with mutual respect and consent in real-life relationships.

- Violent pornography often portrays men as dominant aggressors and women as submissive participants who enjoy acts of humiliation and pain. This can distort young men's understanding of sexual dynamics, making coercion and violence appear normal or even desirable.

- Heavy pornography use has been linked to lower relationship satisfaction and difficulty maintaining emotional connections. Young men who rely on porn for sexual gratification may struggle with real-life intimacy, viewing partners as objects for gratification rather than equals in a mutual experience.[18]

Young women, as well, have been impacted by violent pornography becoming mainstream:

- As violent pornography becomes more mainstream, young women often feel pressured to engage in degrading or painful sexual acts—such as choking, slapping, or rough anal sex—even if they are uncomfortable with them.

- Exposure to violent pornography can distort young women's perceptions of consent, making them believe that discomfort and pain are expected parts of sex. Many report feeling unsure of how to set boundaries, fearing rejection or disappointment from male partners who have been conditioned by pornographic scripts.

- Women in pornography are often portrayed as passive objects meant to satisfy male pleasure. This can lead to additional body image issues and lower self-esteem in young women, who may feel additional pressure to conform to unrealistic beauty standards and sexual performance expectations.[19]

*Young boys' exposure to the manosphere***.** The manosphere is a broad term that refers to a wide variety of men's groups operating on the internet. Generally, the term is used to specifically describe interconnected misogynistic communities. The rise of these groups tracks a disturbing downturn in the wellbeing among young men. Many men and boys are drawn into these spaces

---

[16] *Arizona et al. v. Meta Platforms, Inc., supra*.
[17] "Dr. Vivek Murthy, "Surgeon General: Why I'm Calling for a Warning Label on Social Media Platforms" *New York Times* (Jun. 17, 2024), https://www.nytimes.com/2024/06/17/opinion/social-media-health-warning.html.
[18] *Ibid.*
[19] '*Aggression, strangulation, coercion': The 'concerning' impact of porn on young people.* SBS News, Australia, (Nov. 13, 2024) *accessed at* https://www.sbs.com.au/news/article/aggression-strangulation-coercion-the-concerning-impact-of-porn-on-young-people/bo3wierrq.

when they are in search of solutions to their problems, whether it is social isolation or negative experiences with women, only to be radicalized over time by increasingly extreme content.

Deepfake Pornography. Since its inception, generative artificial intelligence (GenAI) has been used to create nonconsensual pornography, more accurately referred to by sexual assault experts as image-based sexual abuse—almost entirely against women and girls. The widespread availability of GenAI has led to a proliferation of websites and phone-based apps that offer user-friendly interfaces for uploading clothed images of real people to generate photorealistic nude images of not only adults, but also children. According to a recent *New York Times* article:

> Boys in several states have used widely available "nudification" apps to pervert real, identifiable photos of their clothed female classmates, shown attending events like school proms, into graphic, convincing-looking images of the girls with exposed A.I.-generated breasts and genitalia. In some cases, boys shared the faked images in the school lunchroom, on the school bus or through group chats on platforms like Snapchat and Instagram, according to school and police reports.[20]

In February 2024, deepfake nude images of 16 eighth-grade students were circulated among students at a California middle school.[21] Similar reports of abuses, almost always against girls, have been reported across the country and show no sign of abating.[22]

AI Companions. Roughly half of teens report using chatbots, with 24% using them at least weekly and 11% daily.[23] According a recent report from the Minnesota Attorney General, the widespread use of chatbots by teens "has not been accompanied by corresponding safeguards." These products can be "'extremely addictive'" and "researchers have documented that over-usage and addiction are primary risks of personalized chatbots. Several studies have shown that aggregate positive benefits of chatbots are possible, but investigations by journalists and clinicians suggest that these products are not robust in terms of the quality and safety of their responses."[24]

---

[20] Natasha Singer, "Teen Girls Confront an Epidemic of Deepfake Nudes in Schools," *New York Times* (Apr. 8, 2024) *accessed at* https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html.
[21] Mackenzie Tatananni, " 'Inappropriate images' circulate at yet another California high school, as officials grapple with how to protect teens from AI porn created by classmates," *Daily Mail* (Apr. 11, 2024) *accessed at* https://www.dailymail.co.uk/news/article-13295475/Inappropriate-images-California-Fairfax-High-School-AI-deepfake.html.
[22] Tim McNicholas, "New Jersey high school students accused of making AI-generated pornographic images of classmates," CBS News (Nov. 2, 2023) *accessed at* https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/; Lauraine Langreo, "Students Are Sharing Sexually Explicit 'Deepfakes.' Are Schools Prepared?" Ed Week (Sept. 26, 2024) *accessed at* https://www.edweek.org/leadership/studentsare-sharing-sexually-explicit-deepfakes-are-schools-prepared/2024/09; Gabrielle Hunt and Daryl Higgens "AI nudes of Victorian students were allegedly shared online. How can schools and parents respond to deepfake porn?," *The Guardian* (June, 12, 2024) *accessed at* https://www.theguardian.com/australia-news/article/2024/jun/12/ai-nudes-of-victorian-students-were-allegedly-shared-online-how-canschools-and-parents-respond-to-deepfake-porn.
[23] "Minnesota Attorney General's Report on Emerging Technology and Its Effects on Youth Well-Being" (Feb. 2025), p. 28, https://www.ag.state.mn.us/Office/Reports/EmergingTechnology_2025.pdf. ("Minnesota Attorney General's Report").
[24] *Ibid.*

4) **What this bill would do.** The primary purpose of this bill is to protect children from the real harms listed above. According to the author, the status quo of asking businesses to assess children's ages without meaningful accountability is not working for youth. By establishing an age assurance framework in statue, California can protect children while respecting adult access to the internet. In establishing the framework, the current version of the bill requires that manufacturers and application developers do the following for the parents of child device users under 18:

Age assurance signal. Manufacturers of computer devices and operating systems are required to develop an accessible methods for parents to indicate the age and/or birthdate of the primary users of a devices. Once the manufacturer is aware of the age of the user, the device or the operating system must inform an app developer of the age bracket of the user attempting to download their application, using a signal.

Age brackets. If the manufacturer also maintains an online application store, as Apple and Google both do, it would send developers a signal indicating whether the user falls into one of the following age brackets:

- Under five years old
- Five to nine
- 10 to 12
- 13 to 15
- 16 to 17
- Over 18 years old

Parental controls. The bill requires manufacturers to provide parents and guardians the ability to:

- Consent prior to allowing a user under 16 to download an application to their device.
- Connect with the app developer so that the parent may access any parental controls within the application.

A developer who receives a signal indicating that a user is a child, if technically feasible, must provide parents with parental control features. In addition, "as appropriate given the risks that arise from the use of the application" those features must do the following:

- Manage which accounts are linked to their children.
- Manage the delivery of age-appropriate content.
- Limit the amount of time their children spend daily on the application.

Applications covered under the bill. The current definition in the bill covers software applications, online services, products, or features that may be run or directed by a user on a computer, a mobile device, or any other general purpose computing device. This would include, for example, any website the user want to visit, computer program, game, photo editor, and all applications available in an app store.

Enforcement. The bill includes enforcement by the Attorney General and includes an injunction and civil penalties between $2,500 and $7,500 for each impacted child for each violation.

5) **Opposition concerns.** Opponents of the bill raise concerns about the requirement that every application, regardless of how harmless and benign, would be required to develop a way to receive complex signals regarding the age bracket of device users and then create parental controls that the owner of a separate device uses to not only control the downloading of the application but also limit the content and the time the child spends on each application. Regarding this process, Oakland Privacy writes:

> This is an extraordinary amount of complex programming for the huge universe of free and low-cost applications available through the Google Play and Apple stores. It seems obvious that it would a) cause phone applications to be much larger and therefore greatly reduce the number of applications any user could load onto their phone and b) inevitably will result in far fewer free apps for users as costs will significantly rise for creating and maintaining apps. In addition, there is an entire universe of phone apps for which the demands to decode multiple signals, get adult consent and manage content are irrelevant. . . . [Including applications that] have no discernible harmful impacts on minors, but would have to implement this entire scheme under the bill.

Along with the potential technical difficulties associated with the current version of the bill, opponents also raise concerns about language in the bill the leaves developers and parents responsible for determining what constitutes a risk to minors. "While it is important to encourage parental involvement to ensure minor's safety online," Chamber of Progress argues, "parents are not always best suited to control how their child uses a platform." As examples they note that for parents who are not supportive of their child's identity or seek access to certain information, including health information and other online spaces that serve as a "lifeline" for the child.

Of concern are apps that provide critical services such as those supporting mental, physical and reproductive health that offer anonymity. In order for a young person to access those apps, under the current structure of the bill, their parent would be notified and would be required to give consent.

In contrast, the TransLatin Coalition, supporters of the bill, appreciate the balance struck by this bill. They write:

> Many members of our community—both parents and youth—navigate multiple systems with limited resources and information. For immigrant parents, managing their children's online activities can be especially challenging due to language barriers, digital literacy gaps, and long work hours that limit oversight. The Digital Age Assurance Act offers practical solutions that support all parents, including those in our immigrant communities, by creating straightforward, accessible tools for parental oversight through the app store. It eliminates the need for parents to navigate complex settings across dozens of different platforms, provides consistent age verification standards that work across language barriers, and offers parents meaningful involvement without requiring extensive technical knowledge.
>
> Simultaneously, this balanced approach preserves critical online resources for LGBTQ+ youth. For young people in our communities, online spaces often provide essential information and support that may be unavailable in their immediate environments. This is particularly true for trans and gender-diverse youth who may be isolated in their communities or families.

> Unlike approaches in other states that effectively block access to important resources, AB 1043 acknowledges that youth need both protection and access. This balance is especially important for LGBTQ+ youth from immigrant families, who often face multiple layers of marginalization and may have fewer in-person support options.

Regarding allowing app developers and parents to determine what is and is not age appropriate content, Oakland Privacy cautions:

> It is important to note for the record that there is no objective standard in the bill for what constitutes risks to minors and not only does that vary greatly from a five year old to a 17 year old, it also varies greatly from one adult perspective to another.

It seems like these decisions would be made by two entities: a) app developers who would provide some kind of censoring controls and b) parents who would operate those controls. In both cases, the vague term "age appropriate content" could mean many different things. We have seen - and this is not completely absent in the state of California - efforts to ban books from school libraries because they contain gay characters or make references to racism in society or even because they refer to sexual activity. Do we really want a version of Good Reads that censors Judy Blume's *Forever* or *Are You There God, It's Me Margaret*, books literally written to help young girls make sense out of puberty? Let's not forget that although we happily play Jailhouse Rock at 10 year old slumber parties nowadays, at the time some parents wanted the song banned because Presley provoked "lewd feelings" in teenage girls. Age-appropriate is at best a highly subjective term.

6) **Striking a balance between parental control and children's privacy.** In protecting children from the potential harms on the internet, like those discussed previously, there must be a careful balance between appropriate parental control and the rights of older teens to access certain platforms. At the core of this bill is a conceptually elegant solution for establishing the age of the user. By sending an age assurance signal that developers are required to rely on for having actual knowledge of the age of the user, provides a number of significant benefits:

- It alleviates concerns from privacy advocates that age verification would necessarily require everyone to provide developers and platforms with even greater sensitive personal information by having to upload official identification documents in order to prove that they are old enough to access the application or the content.

- It potentially removes the argument from the technology industry that have no definitive way of knowing the age of their users, thus allowing them to avoid responsibility for allowing children to access harmful content. As an example, applications that are restricted to adults generally simply ask the user to attest to whether or not they are old enough to access the site. With an age assurance signal, the platforms would be provided with actual knowledge of the age or age range of the user that they could then rely on to grant or deny access.

- The State's consumer privacy law, the California Consumer Privacy Act, restricts the ability of businesses to be able to use, share, or sell personal information on minors. For those under 13, parental consent is required for the sharing or sale of a child's information, for those older children who are at least 13, but under 16, they must consent to having their personal information shared and sold. However, those restrictions only

apply if a business has actual knowledge of the person's age. An age assurance signal sent to online businesses could provide that actual knowledge.

However, this bill juggles both technical complexity and sensitive issues around parental control and children's privacy and autonomy, raising questions about the right solutions for younger children versus more mature teens.

The author intends to continue working with stakeholders to find the appropriate balance between protecting children from the more dangerous aspects of the internet and preserving their right to both privacy and to access information. As the author continues refining the bill, she may also wish to consider:

- *Defining "device."* While there is currently no definition of device in the bill, under the definition of "covered application store" it references computers, mobile devices, or "any other general purpose computing device." This definition could conceivably cover everything from smartphones and tablets to smart televisions, gaming consoles, fitness devices or other household items. The author may wish to more specifically delineate which devices are intended to be covered.

- *Narrowing the types of applications.* As the opposition noted, the current definition of "application" includes every application and computer program, including those that have no discernable harmful impact. The current definition in the bill would include functional applications such as calendars, to-do-lists, simple games, keyboards, clocks, maps, and weather apps. The author may wish to specifically define which types of applications, computer programs, and websites the bill is intended to cover.

- *Allowing automatic blocking.* There are a number of applications that have already been deemed inappropriate for children under a certain age. For example, Instagram, a social media platform owned by Meta, prohibits children 12 and under from having accounts. In addition, it has restricted accounts for teenagers under 16. As another example, just as with analog pornographic material, minors are prohibited from accessing pornographic websites. Similarly, many AI girlfriend applications are restricted to adults. Rather than going through the process of seeking parental consent for applications that are not appropriate for the age range of the user, and then developing parental controls, the author may wish to require that applications already determined to be inappropriate or unsafe simply be blocked for young users.

- *Considering the appropriate age of consent for downloading applications.* As currently drafted, parental consent is necessary in order for any young person under 16 to download and access any application, no matter how benign. In some instances, the Legislature has established 13 as the age where a young person can provide consent and do not require parental consent. For example, 13-year can decide whether or not they want to opt-in to allowing businesses to share and sell their personal information. In addition, minors 12 and older have the ability to consent to certain medical care, including testing and treatment for sexually transmitted diseases, HIV/AIDs testing, treatment and prevention, and mental health or substance use disorder treatment.[25] Also,

[25] *California Minor Consent and Confidentiality Laws,* National Center for Youth Law (Dec. 2023) https://teenhealthlaw.squarespace.com/california/#consent.

minors of any age can consent to reproductive healthcare, including abortion services and accessing birth control. Finally, beginning this past January, schools districts are prohibited from requiring teachers and other school employees disclose a student's gender identity or sexual orientation to their parents. Prior to any disclosure, the child must first provide their consent. The author may wish to consider aligning the age of requiring parental consent with these other laws, perhaps setting the age at 13 to align with the California Consumer Protection Act.

- *Clarifying the intentions around parental control.* As currently drafted, the bill is unclear in terms of the level and types of parental control that a developer is required to include in their applications and for whom. The following language may benefit from more precision:

    - 1798.501(b)(1) requires that developers "provide readily available features for parents to support a child user's use of the service." Presumably this is intended to require that parents be provided with parental controls. However, it is unclear what is intended by requiring a feature that allows parents to support the user's use of the service.

    - 1798.501(b)(1) also requires that the features allow parents to support their child's use of an application are required to include additional features "as appropriate, *given the risks that arise* [from] use of the application." (Emphasis added.)

    - 1798.501(b)(1)(A) and (C) both require features to "manage" the accounts and access. While these two sections are more easily interpreted, nonetheless, in (A) the feature must "help manage" which accounts are linked to children, raising questions about how this standard is satisfied. Along the same lines, in (C), the developer is required to include a feature that allows the parent to manage the content that is on their child's phone. However, if the author intends for a feature that allows parents to control various features, such as the ability of the account to receive direct messages from unknown people on the platform; determining whether or not the user can access a live chat feature that allows the child to talk directly with other gamers inside an online game; or allowing the child to make in-app purchase, for example, perhaps (C) should state the parental control feature must "allow the parent to control in-app features."

ARGUMENTS IN SUPPORT: The International Centre for Missing and Exploited Children (ICMEC), co-sponsors of the bill, write in support:

> ICMEC views the device-based mechanism outlined in AB 1043 not as a solution that benefits one industry over the other, but rather as the most common sense and feasible solution. It is an industry-wide solution that holds all online services accountable in the online journey of a child.
>
> Rather than providing personal information to dozens of websites and applications, all of which may have varying levels of security and privacy practices, the mechanism in AB 1043 centralizes the point at which age is requested at the lowest common denominator: on the device itself.

> This mechanism is a technically feasible and constitutionally sound method that protects the privacy of both adult and child users. You are not disclosing the identity of a child or adult; once a user enters their age on their device, they are wrapped in a shroud of privacy that provides websites and applications only with a user's age range. This bill will provide a critical tool to protect vulnerable children in California, children whose parents may not be involved or aware of their child's digital experience.

The Source LGBT+ Center writes in support:

> For many LGBTQ+ youth, especially those in rural or conservative areas, online platforms represent their first and sometimes only opportunity to explore their identity, find accurate information, and connect with others who share their experiences. These digital lifelines can mean the difference between isolation and belonging, between despair and hope.
>
> Previous attempts at internet regulation have often threatened these crucial connections through overly restrictive content filters or verification requirements that compromise privacy. We have watched with concern as some legislation has created risks of censorship that disproportionately impact LGBTQ+ content and resources.
>
> AB 1043 takes a fundamentally different approach. By focusing on age verification at the app store level rather than forcing individual platforms to implement their own systems, this legislation protects children without creating unnecessary barriers to accessing important resources.

Also writing in support, California Parents for Public Virtual Education, notes:

> Today's digital landscape was not designed with children in mind, leaving young users vulnerable to exploitation, cyberbullying, and inappropriate content. Research from the Centers for Disease Control and Prevention (CDC) highlights alarming trends, with increasing rates of depression and suicidal ideation among teenagers—particularly young girls—due to online influences.
>
> Parents need effective tools to safeguard their children in an era where digital access is essential for education and socialization.
>
> Assembly Bill 1043 establishes a privacy-first, uniform age verification system, ensuring that app developers and online platforms can implement appropriate safeguards. This legislation empowers parents with greater oversight and creates a responsible framework for businesses to protect young users without compromising innovation or privacy.

ARGUMENTS IN OPPOSITION: In opposition to the bill, TechNet argues:

> AB 1043 requires app store providers to verify the age of users before granting access to app downloads, purchases, or usage. Age verification is a complex challenge to address and requires consideration of how to properly balance the interests of privacy and security. Stringent age verification measures could necessitate the collection, processing, and storage of sensitive personal information, such as birth dates and government-issued identification. This could conflict with data privacy principles like privacy-by-design and data minimization and create new vectors for fraud, as every user in the state must prove whether or not they are a minor.

Additionally, there are privacy concerns associated with the bill's parental consent requirements. Parental consent entails verifying parental relationships and parental rights, which will likely lead to privacy-invasive processes beyond collecting and verifying the age of an individual. For example, even with a birth certificate, there are custody agreements and other issues that could prevent a caregiver listed on that certificate from exercising parental rights to provide consent. Additionally, the bill is silent on the specific methodologies that would be sufficient to obtain and verify parental consent as well as parental relationships and rights, leading to compliance uncertainty and potential legal vulnerabilities.

REGISTERED SUPPORT / OPPOSITION:

Support

Children Now (co-sponsor)
International Centre for Missing & Exploited Children (co-sponsor)
AAPI Equity Alliance
California Parents for Public Virtual Education
Parents for School Options
Parents Support for Online Learning
Protect Our Kids
The Source Lgbt+ Center
The Translatin@ Coalition
1 Individual

Opposition

Chamber of Progress
Oakland Privacy
Technet-technology Network

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200