

Date of Hearing: April 21, 2026

Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

Rebecca Bauer-Kahan, Chair

AB 1856 (Wicks) – As Amended April 6, 2026

SUBJECT: Age verification signals: software applications and online services

SYNOPSIS

AB 1043 (Wicks; Ch. 675, Stats. 2025) enacted the Digital Age Assurance Act (Act), which establishes an age verification system for users of mobile devices and computers. Beginning in 2027, parents who allow their children to be the main users of such devices will be able to configure the device to send a non-identifying age bracket signal – under 13, between 13 and 16, between 16 and 18, or at least 18 – that operating systems and application stores must send to application developers. Developers, in turn, must treat the signal as the primary indicator of the user’s age, thereby ensuring that they can’t turn a blind eye to children on apps intended for more mature audiences.

In signing the law, Governor Newsom noted that streaming services and video game developers had asserted that the bill’s framework is suited to traditional software applications rather than their products. Many of these companies have existing age verification systems in place and must grapple with multi-user accounts shared by families across multiple devices. The Governor urged the Legislature to address these concerns.

This bill seeks to address the Governor’s request by clarifying provisions governing the scope of the bill and circumstances in which a developer may override the age signal because a parent indicates the child has different age information for purposes of that application. The bill would also add data minimization provisions. Finally, the bill would provide that all online spaces where children can access, such as websites, are included within the Act.

The bill is author-sponsored and supported by Children Now and Elevate California, who applaud the extension of last year’s bill. It is opposed by the Motion Picture Association (MPA), who argues the bill doesn’t go far enough to address their concerns, and by Chamber of Progress and TechNet, who express concern about the inclusion of additional online spaces.

Committee amendments set forth in Comment #5 expressly place requirements on applications stores to request and relay the age signal to developers; prohibit covered entities from prompting users to provide different age information; expressly provide that clear and convincing evidence of age information that differs from the age signal imputes actual knowledge of that age range in lieu of the actual knowledge imputed by the age signal; and recast provisions integrating websites into the Act by creating a parallel set of requirements applicable to browser providers and website operators.

EXISTING LAW:

- 1) Establishes the Digital Age Assurance Act. (Civ. Code § 1798.500 et seq.)
- 2) Defines key terms, including:

- a. "Account holder" means an individual who is at least 18 years of age and a parent or legal guardian of a user who is under 18 years of age in this state.
 - b. "Age bracket data" means nonpersonally identifiable data derived from a user's birth date or age for the purpose of sharing with developers of applications that indicates the user's age range, including, at a minimum, whether the user is under 13, between 13 and 16, between 16 and 18, or at least 18.
 - c. "Covered application store" means a publicly available internet website, software application, online service, or platform that distributes and facilitates the download of applications from third-party developers to users of a computer, a mobile device, or any other general purpose computing that can access a covered application store or can download an application.
 - d. "Developer" means a person that owns, maintains, or controls an application.
 - e. "Operating system provider" means a person or entity that develops, licenses, or controls the operating system software on a computer, mobile device, or any other general purpose computing device.
 - f. "Signal" means age bracket data sent by a real-time secure application programming interface or operating system to an application.
 - g. "User" means a child under the age of 18 that is the primary user of the device.
(§ 1798.500.)
- 3) Requires an operating system provider to do all of the following:
- a. Provide an accessible interface at account setup that requires an account holder to indicate the birth date, age, or both, of the user of that device for the purpose of providing a signal regarding the user's age bracket to applications available in a covered application store.
 - b. Provide a developer who has requested a signal with respect to a particular user with a digital signal via a reasonably consistent real-time application programming interface that identifies whether the user is under 13, between 13 and 16, between 16 and 18, or at least 18.
 - c. Send only the minimum amount of information necessary to comply with the Act and not share the digital signal information with a third party for a purpose not required by the Act. (§ 1798.501(a).)
- 4) Requires developers to request a signal with respect to a particular user from an operating system provider or a covered application store when the application is downloaded and launched.
- a. Deems a developer that receives a signal to actual knowledge of the user's age range.
 - b. Prohibits a developer from willfully disregarding internal clear and convincing information otherwise available to the developer that indicates the user's age is different than the signal indicates.

- c. Requires a developer to treat a signal as the primary indicator of a user's age range unless the developer has internal clear and convincing information that the user's age differs from that indicated by the signal, in which case the developer must use that information as the primary indicator of the user's age.
 - d. Prohibits a developer that receives an age signal from requesting more information from an operating system provider or a covered application store than the minimum amount of information necessary to comply with the Act, and from sharing the signal with a third party not required by the Act. (§ 1798.501(b).)
- 5) Requires an operating system provider, with respect to a device for which account setup was completed before January 1, 2025, to provide an accessible interface that allows an account holder to indicate the birth date, age, or both, of the user of that device for the purpose of providing a signal regarding the user's age bracket to applications available in a covered application store. (§ 1798.502(a).)
 - 6) Requires a developer, if the application is updated on or after January 1, 2026, or downloaded before January 1, 2027, to request a signal from a covered application store with respect to a user of the device before July 1, 2027. (§ 1798.502(b).)
 - 7) Subjects violators to civil penalties for each affected child of up to \$2,500 for negligent violations and \$7,500 for intentional violations, in an action brought by the Attorney General. Excuses operating system providers and covered application stores from liability for erroneous signals and conduct by developers that receive signals, if the operating system provider or covered application store makes a good faith effort to comply with the Act. (§ 1798.503.)

THIS BILL:

- 1) Expands the definition of "application" to include an online service, product, or feature. Excludes broadband internet access services, telecommunications services, and delivery or use of a physical product from those newly added categories.
- 2) Deletes the definition of "user" and clarifies that the obligations of the Act apply with respect to child users who are the primary users of the device. Clarifies that the definition of "signal" pertains only to the primary user of a device.
- 3) Specifies that the requirement of an operating system provider to provide an accessible interface applies only if the operating system provider's operating system has an account setup feature with respect to the use of the operating system on a particular device.
- 4) Requires operating systems to send only the minimum amount of the information necessary to comply with the Act.
- 5) Provides that "clear and convincing information" includes, but is not limited to, age information shared with a developer by an account holder regarding the age of a user of a subaccount of the primary account of the account holder.
- 6) Makes other clarifying and conforming changes.

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

Last year's bill, AB 1043, creates a consistent, privacy-first pathway to online age assurance — giving families the confidence that tech platforms can build the right protections for kids into their products without interfering with an app's existing account features, user settings, or ability to set parental controls. This age assurance framework establishes actual knowledge of users' age range in order for these applications to abide by applicable laws, including California's groundbreaking privacy laws. AB 1856 would clarify provisions in order for applications and operating system providers to work within this framework of age assurance. In addition, we also want to ensure that all online spaces where children can access, such as websites, are included within this age assurance framework and can comply with applicable laws.

2) The Digital Age Assurance Act. The internet was not designed with children in mind. It was built as an open, anonymous network in which every user is presumed to be an adult, absent affirmative evidence to the contrary — a default assumption that platforms have inherited and, for the most part, maintained. The practical consequence is that the burden of identifying minors — whether to prevent them from accessing age-inappropriate content, or to provide additional privacy protections — must be addressed through additional mechanisms that involve significant tradeoffs and vary considerably in their rigor and cost. The simplest — asking users to enter a birth date or check a box — imposes virtually no burden on anyone but provides no real verification; a minor willing to misrepresent their age can do so with ease. Documentary verification is more reliable, but it requires users to transmit sensitive identity documents to potentially dozens of platforms, creating serious privacy and data security risks, and it disadvantages those segments of the population — including many adolescents — who lack qualifying documents in the first place. Algorithmic and biometric methods, including inferring age from behavior, device signals, or facial analysis, avoid the documentation problem but demand expansive data collection. These methods also perform unreliably at precisely the age boundaries that matter most, and can be circumvented.

AB 1043, which enacted the Digital Age Assurance Act (Act), sought to achieve a better path forward by creating a system of privacy-protective age verification. Under the Act, operating system providers must provide an accessible interface at account setup that requires an account holder (parent) to indicate the birth date, age, or both, of the user (a child that is the primary user) of that device for the purpose of providing a signal regarding the user's age bracket — under 13, between 13 and 16, between 16 and 18, or at least 18 — to applications available in a covered application store. App developers are required to request signals from application stores and operating system providers when the app is downloaded or launched. Developers who receive signals are deemed to have actual knowledge of the user's age range and must treat the signal as the primary indicator of age, unless they have clear and convincing internal information showing the signal is inaccurate.

3) This bill clarifies the Act and expands it to include websites. *Responds to the Governor's request to address streaming services.* In signing AB 1043, Governor Newsom noted that streaming services and video game developers had asserted that the bill's framework is suited to traditional software applications rather than their products. Many of these companies have

existing age verification systems in place and must grapple with multi-user accounts shared by families across multiple devices. The Governor urged the Legislature to address these concerns.

Rather than carve out such services, the author is seeking to address these issues holistically by finding broadly applicable solutions. To this end, the bill deletes the definition of “user” and clarifies that the obligations of the Act apply with respect to child users who are the primary users of the device. In cases involving multiple subaccounts on shared devices, the child will be unlikely to be the primary user of the device. The bill also clarifies that the definition of “signal” pertains only to the primary user of a device. Additionally, the bill provides that “clear and convincing information” includes, but is not limited to, age information shared with a developer by an account holder regarding the age of a user of a subaccount of the primary account of the account holder.

Data minimization. The bill expressly requires operating systems to send only the minimum amount of the information necessary to comply with the Act.

Adds websites to the Act’s framework. When AB 1043 passed this Committee last year on a 13-0 vote, it defined “application” to include any “online service, product, or feature” – thereby covering websites and other online products and features. Later in the process, due to technical and policy complications, the author narrowed the bill to apply only to app developers with the intent to address the issue of websites later.

This bill again defines “application” to include an online service, product, or feature. The bill excepts from those newly added categories, broadband internet access services, telecommunications services, and delivery or use of a physical product. However, because this method of incorporating websites has raised some drafting questions, the author has opted to address this issue by creating a parallel scheme that applies to browsers and websites. Those amendments are described in more detail in Comment #5.

Scoping. The bill additionally specifies that the requirement of an operating system provider to provide an accessible interface applies only if the operating system provider’s operating system has an account setup feature with respect to the use of the operating system on a particular device. This ensures that operating systems that do not or are unable to provide such features are not subject to the Act.

4) Opposition concerns. In a detailed memo, the Motion Picture Association (MPA) argues (1) the Act effectively prohibits applications from relying on their internal data, and (2) the Legislature should permit developers to direct operating system providers to block downloads for minors.

As to the first argument, MPA points to a draft issuing in the Act: Once a developer is provided with an age signal, they are deemed to have actual knowledge and must treat that signal as the primary indicator of age. If, however, there is clear and convincing information to the contrary, the developer must treat that age information as the primary indicator of age. But the statute is silent as to whether the developer is still considered to have actual knowledge based on the age signal. MPA argues the issue should be resolved for streaming services by allowing “family account applications” that *offer* subaccounts to verify age based on internal data rather than the age signal.

However, MPA's solution would work only for a subset of developers. In lieu of a carveout, the author has opted to simply clarify the intent: once the developer has clear and convincing information of an age range that differs from that in the age signal, the developer should be deemed to have actual knowledge of the new age range in lieu of the age range indicated by the signal.

As to the second argument, MPA asserts that developers should be able to signal to application stores that they do not want their application accessed by minors, obviating the need to comply with the Act. Although there is some appeal to this point when it comes to applications that, for example, display adult-only content, in practice this exception would sweep far more broadly: any developer who does not want to deal with legal compliance related to minors would have the option to bar minors, severely limiting their access to valuable content and removing the decision from families.

Separately, TechNet writes in opposition to the bill's extension to any "online service, product, or feature":

This raises important questions regarding how such requirements would be operationalized in practice. Unlike applications, which exist within defined distribution and compliance ecosystems, online services do not have a clear or uniform mechanism for implementing these obligations. As a result, it is unclear how entities would determine when and how to comply, or how such requirements would be enforced consistently.

We are particularly concerned that this expansion would apply new obligations to a broad and diverse set of services before the underlying compliance infrastructure has been fully developed or tested under existing law. This creates a risk of uncertainty for both providers and users, and may result in unintended consequences for product functionality and user experience.

Given the scale of this proposed expansion, we believe additional clarity is needed regarding how these requirements would apply to websites and other online services, and how compliance would be achieved in a consistent and workable manner.

As discussed below, amendments omit reference to "online service, product, or feature" and instead directly integrate websites. Going forward, the author has indicated an intent to work closely with stakeholders to ensure compliance can be achieved in a consistent and workable manner.

5) Amendments. Committee amendments set forth below (1) expressly place requirements on applications stores to request and relay the age signal to developers (a clear implicit requirement of the Act); (2) expressly provide that clear and convincing evidence of age information that differs from the age signal imputes actual knowledge of that age range in lieu of the actual knowledge imputed by the age signal; (3) prohibit covered entities from prompting a user to provide different age information; and (4) recast provisions integrating websites into the Act by creating a parallel set of requirements applicable to browser providers and website operators, wherein browser providers serve as intermediaries that request and relay the age signal to website operators that are otherwise required by law to verify age. It is anticipated that this change will necessitate further refinement with stakeholder feedback to ensure technical feasibility.

The amendments are as follows:

1798.500. For the purposes of this title:

(a) (1) “Account holder” means an individual who is at least 18 years of age or a parent or legal guardian of a user who is under 18 years of age in the state.

(2) “Account holder” does not include a parent of an emancipated minor or a parent or legal guardian who is not associated with a user’s device.

(b) “Age bracket data” means nonpersonally identifiable data derived from a user’s birth date or age for the purpose of sharing with developers of applications that indicates the user’s age range, including, at a minimum, the following:

(1) Whether a user is under 13 years of age.

(2) Whether the user is at least 13 years of age and under 16 years of age.

(3) Whether the user is at least 16 years of age and under 18 years of age.

(4) Whether the user is at least 18 years of age.

(c) “Application” means a software application ~~or online service, product, or feature~~ that may be run or directed by a user on a computer, a mobile device, or any other general purpose computing device that can access a covered application store or download an application.

(x) “Browser” means an application that enables a user to visit a website.

(x) “Browser provider” means a person or entity that controls or operates a browser for use on a computer, mobile device, or any other general purpose computing device.

(d) “Child” means a natural person who is under 18 years of age.

(e) (1) “Covered application store” means a publicly available internet website, software application, online service, or platform that distributes and facilitates the download of applications from third-party developers to users of a computer, a mobile device, or any other general purpose computing that can access a covered application store or can download an application.

(2) “Covered application store” does not mean an online service or platform that distributes extensions, plug-ins, add-ons, or other software applications that run exclusively within a separate host application.

(f) “Developer” means a person that owns, maintains, or controls an application.

~~(g) “Online service, product, or feature” does not mean any of the following:~~

~~(1) A broadband internet access service, as defined in Section 3100.~~

~~(2) A telecommunications service, as defined in Section 153 of Title 47 of the United States Code.~~

~~(3) The delivery or use of a physical product.~~

(h) “Operating system provider” means a person or entity that develops, licenses, or controls the operating system software on a computer, mobile device, or any other general purpose computing device.

(i) “Signal” means age bracket data that pertains to the primary user of a device ***that is either of the following:***

(A) Sent by a real-time secure application programming interface or operating system to an application.

(B) Communicated by a browser provider to a website operator in any technically feasible manner.

(x) “Website operator” means a person that owns, maintains, or controls a website that is subject to a law that requires the website operator to verify the age of users.

SEC. 2. Section 1798.501 of the Civil Code is amended to read:

1798.501. (a) If an operating system provider’s operating system has an account setup feature with respect to the use of the operating system on a particular device, an operating system provider shall do all of the following:

(1) Provide an accessible interface, at account setup, that requires an account holder to indicate the birth date, age, or both, of the primary user of that device for the purpose of providing a signal regarding the primary user’s age bracket to ~~applications available in a covered application store~~ ***all of the following:***

(A) A covered application store.

(B) A developer.

(C) A browser provider.

(D) A website operator.

(2) Provide a developer, ***a covered application store, or a browser provider*** who has requested a signal with respect to a particular user with a digital signal via a reasonably consistent real-time application programming interface that identifies, at a minimum, which of the following categories pertains to the user:

(A) Under 13 years of age.

(B) At least 13 years of age and under 16 years of age.

(C) At least 16 years of age and under 18 years of age.

(D) At least 18 years of age.

(3) Send only the minimum amount of information necessary to comply with this title.

(b) An operating system provider shall not share the digital signal information with a third party for a purpose not required by this title.

(c) (1) A covered application store shall do both of the following with respect to a user of the covered application store:

(A) Request a signal from the user's operating system provider.

(B) Provide the signal received pursuant to subparagraph (A) to a developer upon request.

(2) A browser provider shall do both of the following with respect to a user of the browser:

(A) Request a signal from the user's operating system provider.

(B) Provide the signal received pursuant to subparagraph (A) to a website operator upon request.

(de) (1) (A) A developer shall request a signal with respect to a particular user from an operating system provider or a covered application store when the application is downloaded onto, and launched from, a particular device.

(B) A website operator shall request a signal with respect to a particular user from the user's browser provider when the user accesses the website.

(C) An entity subject to this title shall not prompt the user to change the user's age information.

(2) (A) A developer ***or website operator*** that receives a signal pursuant to this title shall be deemed to have actual knowledge of the age range of the user to whom that signal pertains when the user accesses the application ***or website*** from the device referenced in paragraph (1) even if the developer ***or website operator*** willfully disregards the signal.

(B) A developer ***or website operator*** shall not willfully disregard internal clear and convincing information otherwise available to the developer ***or website operator*** that indicates that a user's age is different than the age bracket data indicated by a signal provided by an operating system provider, ~~or a~~ covered application store, ***or browser provider***.

(3) (A) Except as provided in subparagraph (B), a developer ***or website operator*** shall treat a signal received pursuant to this title as the primary indicator of a user's age range for purposes of determining the user's age.

(B)-(i) If a developer ***or website operator*** has internal clear and convincing information that a user's age is different than the age indicated by a signal received pursuant to this title, the

developer *or website operator* shall use that information as the primary indicator of the user’s age *and, notwithstanding subdivision (d)(2)(A), shall be deemed to have actual knowledge of the age range of the user to whom that information pertains.*

(iii) As used in this subparagraph, “clear and convincing information” includes, but is not limited to, age information shared with a developer *or website operator* by an account holder regarding the age of a user of a subaccount of the primary account of the account holder.

(4) A developer *or website operator* that receives a signal pursuant to this title shall use that signal to comply with applicable law but shall not do either of the following:

(A) Request more information from an operating system provider, ~~or a~~ covered application store, *or website browser* than the minimum amount of information necessary to comply with this title.

(B) Share the signal with a third party for a purpose not required by this title.

The amendments will also include necessary conforming changes, including integrating browser providers and website operators into the Act’s liability scheme, as well as any other technical, nonsubstantive changes recommended by the Office of Legislative Counsel.

ARGUMENTS IN SUPPORT: Elevate California writes:

Just like we have age restrictions for driving, buying cigarettes, and buying alcohol, age limitations may end up being appropriate to protect minors from online harms. This bill builds on prior California legislation, the Digital Age Assurance Act, AB 1043 (Wicks) of 2025 to require age verification upon device setup that can later be used when the device (rather than the “user”) downloads applications and services. Assembly Bill 1043 or 2025 doesn’t come into full effect until 2027. We need to coordinate in order to protect children from online harms and protect them from marketers using their data to manipulate and sell to them. These are reasonable restrictions in line with other reasonable age based restrictions for our children.

ARGUMENTS IN OPPOSITION: Taking an oppose-unless-amended position, MPA writes:

[. . .] MPA appreciates that this Bill makes clarifications to the law that partially address the concerns raised by MPA with respect to “family account”-style applications that are shared by multiple members of a household and accessed across multiple devices. However, the Bill does not fully address the implementation challenges that the law creates for services, like many streaming services, which seek to rely on their own customer data. Additionally, the Bill mandates that developers request and process age data for any minor that wants to download their application *even if* the developer has determined not to make their application available to minors. This needless exchange of minors’ data does nothing to advance the law’s policy goals.

MPA supports the goal of creating a safe online ecosystem for children. Indeed, MPA is an industry leader in providing parents with the necessary tools to make informed decisions about what content their children can access—including with its gold-standard content

ratings system for motion pictures. However, the Bill does not adequately address the law's implementation problems. [. . .]

REGISTERED SUPPORT / OPPOSITION:

Support

Children Now
Elevate California

Opposition

Chamber of Progress
TechNet-technology Network

Oppose Unless Amended

Motion Picture Association

Analysis Prepared by: Josh Tosney / P. & C.P. / (916) 319-2200