California Takes Action on Youth Online Safety: FAQs on the Digital Age Assurance Act

Alysa Z. Hutnik, Laura Riposo VanDruff, Alexander I. Schneider, Salim Rashid

October 21, 2025

With the Digital Age Assurance Act, California charts an alternate path for youth safety on the internet.

On October 13, 2025, California Governor Gavin Newsom signed AB 1043, the Digital Age Assurance Act, into law.

The Big Tech-supported measure, which takes effect on January 1, 2027, adopts an app-store centric age assurance model, where the operating system providers (think: Apple iOS, Google Android) are responsible for communicating age signals to app developers upon request. The new law follows a recent trend of shifting away from age checks on individual sites or services (and the attendant data security risks that have resulted, exemplified most recently by the Discord data breach that exposed 70K photo IDs) and towards a model that relies on age checks at the operating system level.

Even so, California has charted a new path with AB 1043. Unlike similar age assurance legislation enacted earlier this year in states like Utah and Texas, the new California model shifts significant compliance obligations away from the operating system and to the app developer, while also dispensing with the other laws' more rigid age verification and parental consent frameworks in favor of a self-reported model.

The result is a compromise bill that was reported to garner support from Big Tech companies that had opposed the earlier initiatives in Utah and Texas. That's no small feat, particularly as the Texas law, the Texas App Store Accountability Act, faces a new legal challenge as the Computer & Communications Industry Association (CCIA) recently brought a lawsuit asking a federal judge to strike down the law as unconstitutional.

In his signing statement, Governor Newsom recognized that streaming providers opposed the bill because they already provide age-appropriate user experiences via user profiles, but argued that the California Legislature had sufficient time to address these concerns in the 2026 legislative session. According to Politico, Assemblymember Buffy Wicks, the sponsor of AB 1043, has signaled she is open to working with streaming providers on a potential fix in the coming year.

Here's additional detail on AB 1043's requirements for operating system providers and app developers.

What does this law require for operating system providers?

AB 1043 requires an operating system provider—defined as "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"—to provide an interface at account setup that prompts the account holder to indicate the birth date or age of the user of the device. For example, an account holder might provide their own age if they are the user of the device, or they might provide the age of a member of their household who will use the device.

Importantly, the California law does not require the operating system provider to verify the age. Rather, the operating system provider must provide a developer who requests the age signal with the device user's age range based solely on the information provided by the account holder.

The age ranges that the operating system provider may report to the developer are: under 13 years of age, 13 to under 16 years of age, 16 to under 18 years of age, or at least 18 years of age. The operating system provider may not share the age signal with a third party for a purpose not required by AB 1043.

What does this law require for developers?

Under the new California law, application developers must request an age signal from the operating system provider or app store when the developer's app is downloaded and launched. The developer must treat the age signal as the "primary indicator" of the user's age unless there is "clear and convincing" information that the age is different, in which case the developer may use the alternate age data as the primary indicator of the user's age.

The new law defines a "developer" somewhat circuitously. A developer is a person that "owns, maintains, or controls" an application. An "application," in turn, is defined as a "software application 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." Notably, this definition does not require that the app be downloadable from an app store as long as the app can be downloaded to the user's device some other way.

A "covered application store" includes software or a website that distributes and facilitates the download of third-party apps, but explicitly omits the distribution of extensions, plug-ins, add-ons, or other software applications that run exclusively within a separate host application (e.g., browser plugins).

Does this law mandate formal age verification?

No. Rather than mandate a formal age verification, where the user would need to present a government-issued ID or prove their age in some other commercially available fashion, AB 1043 merely requires the account holder to "indicate" the birth date or age of the user of the device.

This approach stands in stark contrast to the Utah and Texas models. For example, under the Utah App Store Accountability Act, which takes effect May 6, 2026, the app store provider must request age information and verify the age information using "commercially available methods that are reasonably designed to ensure accuracy," or an age verification method adopted by forthcoming rulemaking. The Texas law, effective January 1, 2026, also requires the use of a "commercially reasonable method of verification" to verify the user's age.

Does this law mandate parental consent for a child to download an app?

A developer that receives an age signal is deemed to have "actual knowledge" of a user's age range under AB 1043, but the law does not specify how a developer should respond to this age information. For example, the law does not create a new parental consent requirement similar to the Utah or Texas models. Rather, the law makes clear its protections are "in addition to those provided by any other applicable law," requiring that its provisions be interpreted together with the California Consumer Privacy Act (CCPA) and the currently enjoined California Age-Appropriate Design Code Act.

As a practical matter, then, AB 1043's "actual knowledge" scheme shifts liability to the app developer to determine how to respond to an age signal in accordance with its legal obligations. For example, developers with actual knowledge that they are engaging with a child under 13 would face COPPA requirements, and developers with actual knowledge that they are engaging with a teen under 16 would face sale/sharing consent obligations under CCPA.

The actual knowledge imputed to the developer extends "across all platforms of the application and points of access of the application." This broad scope suggests that developers may be expected to consider age information that the developer receives with respect to a particular device even when engaging with a user on a different device.

This focus on developer compliance rejects a key feature of the Texas and Utah laws that requires app stores to police app downloads, preventing minors from downloading apps without parental consent. The Texas and Utah laws also require consent from the parent prior to making "significant changes" to apps, to give parents an opportunity to consent to their child's use of the app as modified (including, for example, if monetization functionality is added to an app). The California law fully rejects this overall parental consent scheme.

How is liability and enforcement structured in AB 1043?

AB 1043 provides strong liability protections for the operating service provider. For example, the law states that an operating service provider or covered application store that "makes a good faith effort to comply … shall not be liable for an erroneous signal indicating a user's age range or any conduct by a developer that receives a signal indicating a user's age range." No such liability shield is available in AB 1043 for the application developer.

The new law also states that there is no liability for the operating system provider, app store, or developer when a device is used by a person who is not the user associated with the age signal.

The law is enforceable by the California Attorney General with statutory penalties of up to $2,500 per affected child for a negligent violation of the law and $7,500 per affected child for an intentional violation. The Utah and Texas laws include private rights of action pursuant to their state consumer protection laws.

Is there any litigation challenging app store age verification laws?

On Thursday, October 16, 2025, CCIA brought a lawsuit for declaratory and injunctive relief in federal court challenging the Texas App Store Accountability Act. CCIA argues in part that the Texas law is unconstitutional because it targets access to protected speech, is an unconstitutional prior restraint on speech rights, and impermissibly compels app stores and app developers to speak. We'll continue to monitor the new case.