Hashed & Salted | A Privacy and Data Security Update
December 2025

App Store Age Verification Laws Trigger New Federal and State Children's Privacy Requirements

Starting in January, three state app store age verification laws will take effect: Texas' App Store Accountability Act (effective Jan. 1), Utah's App Store Accountability Act (effective May 7) and Louisiana's App Store Accountability Act (effective July 1). California's app store age verification law—AB 1043, the Digital Age Assurance Act, passed in September, will take effect Jan. 1, 2027. Several other states across the country, including Alabama, Florida, New York and Ohio, introduced age verification legislation in 2025. Earlier this year, app store laws made the jump from state to federal when Sen. Mike Lee, R-Utah, and Rep. John James, R-Mich., introduced the App Store Accountability Act, a federal version similar to the state laws that would preempt those state laws.

While the names of these laws would suggest that they are focused on regulating app stores, they also impose significant obligations on app developers, including affirmative requirements to designate suitable age range categories for their apps and to incorporate application programming interfaces (APIs) to ingest and process the age ranges and parental consents of applicable users collected by the app stores. If an app developer is advised by an app store that one of its users is a minor, the Utah and Louisiana laws specifically require the app developer to comply not only with children's privacy laws that may protect minor users but also with the app developer's own guidelines for minor users in its privacy policy and terms of use. By implicating the patchwork of children's privacy laws in the United States, this legislation has a potentially far-reaching impact—especially for operators of general audience sites that have previously been unaware of the ages of their users and therefore believe that they are not covered by children's privacy laws.

Below is an overview of the requirements and legal implications of these new laws for app developers, along with guidance for some best practices on how to comply with the laws.

Age Rating of Apps and Purchases Within the Apps

App developers are required to provide app stores with a designated age range not only for their applications but also for all the purchases that can be made on their apps. All the state laws apply the same age ranges and designations: younger than 13 = child; 13 – 15 = younger teen; 16 – 17 = older teen; and 18 and over = adult. In addition to the designation, app developers must provide the reason for the designated age range.

Age range designations for apps and purchases must be accurate; a misleading age range is one of the few specific violations for app developers under these laws. While none of the state laws specifically describe how an app developer should determine the age range of their app, the laws in Utah and Louisiana state the age range should provide "an assessment of the suitability" for that

Attorney Advertising

age group. In the past, app store age ratings were based predominantly on content; the age ratings did not focus on either the apps' privacy policies or the declared age ratings in those privacy policies and terms of use. Given the broad description of "suitability" for children and the potential for liability if the designated age range is incorrect, all app developers should reassess their app store age range category and consider matching the age range, if any, published in their privacy policy and terms of use.

At this time, neither Google nor Apple has publicly announced a new mechanism for app developers to update the age range categories for apps or app purchases in order to comply with the new laws. Therefore, app developers may have to proactively update those categories by contacting the app stores and using the traditional processes for updating an app's age range to be in compliance with these laws.

Age Verification

Under the new laws, app stores must develop a method for new account holders in the designated states to verify their age and age category, and then communicate that age category to the app developer. In October, both Google and Apple announced the launch of new APIs that will allow apps to receive a user's age range and supervision status. Google launched the New Play API and Apple launched its Declared Age Range API. The app store accountability laws require app developers not only to incorporate these APIs but also to verify the age category of the users through these APIs. Incorporating these APIs is critical for app developers because all the state laws provide a safe harbor from certain violations if the app developers have properly implemented these APIs and are using the age verification shared through them.

In addition to implementing these APIs, app developers must incorporate processes for ingesting the information from the app stores and ensuring that the app enforces any legally required age-related restrictions on users that it now knows may be under the age of 13, 16 or 18. All the laws allow the app developers to use the age ranges to implement any developer-created, safety-related features or defaults and enforce the app developers' own age-related restrictions contained in their privacy policies and terms of use. More importantly, the Utah and Louisiana laws require app developers to enforce these legally required or developer-created age-related restrictions.

Finally, all three of the state laws coming into effect in 2026 prohibit the use of the information shared through the APIs for any purpose other than age verification, and the Texas law requires app developers to delete the information upon completion of any age verification processes. App developers must therefore have an established process for siloing any data obtained through the APIs to ensure that it is only used for age verification and deleted after it is used for that purpose.

Parental Consent

Under all the laws, app stores are responsible for obtaining parental consent before allowing a minor to download an app, purchase an app or make a purchase within an app. Based on the information released by Google and Apple, Google will obtain the consent through its Play Console feature and Apple will obtain the consent through the Family Sharing Group. If Google or Apple obtains consent from the parent, each intends to inform the app of the consent through the API.

Google has indicated that if a parent does not consent to a download or purchase, the app store will not allow the minor to complete the download or purchase. Apple likely will do the same. While neither Google nor Apple has specifically confirmed this, it appears that the app stores will not share a minor's age category until the parent has consented to the download or purchase. The app stores also are required to allow parents to revoke consent, which will be sent to the app developer through the Google or Apple API. App developers must therefore have processes in place to act upon a revocation of consent, which may require the app developer to delete any personal information related to the child.

Providing Notice of Significant Changes

App developers are required under all the state laws to notify the app store of any significant changes to an app's terms of use or privacy policy. In all three laws, significant changes are defined as changes that:

- Change the type or category of personal data collected, stored or shared by a developer
- Affect or change the rating assigned to the app

- Add new monetization features to the app, including new opportunities to make a purchase in or use the app or new advertisements in the app
- Materially change the functionality of user experience of the app

After the app developers notify the app store of the significant change to the app's terms of use or privacy policy, the app store must notify parents of the change and obtain parental consent for minors to continue to use or purchase the app. If parents revoke consent, app developers must have processes in place to comply with the parents' wishes, which may include not allowing the minor to use the app or make a specific purchase.

Further Implications of the App Store Accountability Acts

Because app stores will now be providing the age category of its users in Texas, Louisiana and Utah, and because at least two of the laws specifically require app developers to comply with all legal age restrictions and app restrictions, the app store accountability acts may inadvertently trigger new requirements for app developers under federal and other state privacy laws. For instance, app developers may have previously assumed that all their users were adults but now will have actual knowledge that at least some of them are minors (under 18, 16 or 13).

The Children's Online Privacy Protection Act (COPPA)

If an app developer has actual knowledge that a child is under the age of 13 because the app store has given the app developer the child's age, the app developer will now have to comply with COPPA for that user, including deleting any personal information it had previously collected from the child. If the app developer intends to collect any personal information from the user, then the app developer will have to obtain verifiable parental consent, unless it falls under any of the COPPA exceptions for the collection of personal information from a child without verifiable parental consent.

If a significant number of an app's users are under the age of 13, the app developer may be required to reassess its classifications under COPPA's four general classifications of online services: (1) online services primarily directed toward children, which require verifiable parental consent for all users prior to the collection of any personal information; (2) online services directed toward children, which allow app developers to age-gate and only seek verifiable parental consent from users who identify themselves as under the age of 13; (3) mixed audience sites, which are treated the same as online services directed toward children; and (4) general audience sites, which do not need to age-gate and can collect personal information from users without ever obtaining verifiable parental consent. Many sites consider themselves general audience sites. If a general audience site discovers that a substantial portion of its users in a specific state are under the age of 13, that knowledge likely would make the site a mixed audience site that would have to age-gate prior to the collection of personal information. After Jan. 1, app developers should closely monitor how many of their users fall into the under 13 age category.

State Laws

The collection of a user's age range from the app store may also trigger other state privacy laws. Multiple states, including Texas, have privacy laws that may consider a child's personal information "sensitive information." Under the Texas Data Privacy and Security Act, a child's personal data is sensitive data that cannot be processed without first obtaining parental consent. Once an app developer knows that a user is under the age of 13, it can no longer process that user's information. In addition, some states have laws with restrictions related to teen users, such as requiring opt-ins or prohibiting the use of teens' personal information for targeted advertising. App developers also will have to comply with these state laws.

In addition to these state laws related to the sharing of information of specific minor users, knowledge that a significant number of users are minors may trigger other children's privacy laws, such as age-appropriate design codes. Similar to COPPA, these state laws are triggered simply if it is likely that the apps are used by minors.

Complicating this analysis is the new complaint by the Florida attorney general against the operator of a streaming platform for smart TVs for collecting and selling children's information in violation of the Florida Digital Bill of Rights. The attorney general argues in the complaint that the platform had "actual knowledge" that children were using its services based on the fact that it offered

children's content and apps on its service. The attorney general did not put forth any evidence that the platform had knowledge that children—not parents—were using its services, nor did the attorney general have any specific demographic information that children were using the services. Instead, the complaint alleges that the platform provided children's content, that many households have children under the age of 18 and that the platform was trying "to escape liability by feigning ignorance about its underage users." The fact that operators of similar apps will have demographic information about their specific users increases the risk of litigation against app developers under these types of state privacy laws.

What's Next?

Since the passage of COPPA, many online services have avoided COPPA compliance by arguing that they are general audience sites. Even if these online services were aware that some of their users were minors, they were able to avoid compliance by claiming they did not have actual knowledge of the users' ages because they don't ask users for their age or birth year. With these new app store accountability laws taking effect, app developers will have actual knowledge of their users' ages, which may require them not only to treat individual users as children but also to classify their apps as mixed audience sites. To avoid violating these new laws, as well as existing state and federal laws, app developers must not only integrate the Google and Apple APIs but also develop processes to ensure that their collection and use of the personal information of minors complies with all the laws that protect minors' privacy.

A To-Do List for All App Developers:

- Reassess your app's age category and update it on the app stores.
- Integrate the Google and Apple APIs.
- Develop and implement processes for handling minor users identified through the Google and Apple APIs.
- Silo any information collected from the Google and Apple APIs to ensure that it is only used for age verification purposes.
- Establish processes for when parents revoke previously given consent.
- Establish processes for notifying the app stores if privacy policies or terms of use have been materially changed.
- Determine, based on information shared from the app stores, whether your app will have to comply with COPPA or state privacy laws that apply to websites that are directed toward children.
- Determine, based on information shared from the app stores, whether the app can still collect personal information from the user under state and federal privacy laws and the app's own privacy policies and terms of use.

Related Professional

Nerissa Coyle McGinn . . . . . nmcginn@loeb.com

This is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This publication does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

© 2025 Loeb & Loeb LLP. All rights reserved. 8164 REV1 122925