

# State App Store Accountability Acts Introduce New Obligations for App Developers

October 16, 2025

**UPDATE:** On December 23, 2025, a federal judge issued a preliminary injunction blocking the Texas App Store Accountability Act from taking effect on January 1, 2026. Please contact the authors for the most up-to-date status.

New state laws aimed at age verification and parental consent for online apps will take effect in 2026, imposing significant compliance obligations and raising enforcement risks for app developers as well as app stores. Texas, Utah, and Louisiana have enacted versions of App Store Accountability Acts (ASAAs), which establish specific requirements for app developers and stores, and may be enforced in some cases by private litigation.

These laws are aimed at expanding online age-gating and applying parental consent requirements even to apps that are not “directed” to children under 13 under federal privacy law. As a result, the laws will impact app developers that do not intend for children to use their apps and do not typically need to handle age-related information about their app users. Any business offering an app to a resident of these states – regardless of its targeted audience – should be prepared to comply with their obligations before the fast-approaching deadlines.

## Core Developer Obligations

While these three laws share common compliance themes, they contain nuanced differences that complicate any one-size-fits-all approach. Developers must carefully examine the specific requirements of each state’s law. In general, the laws require the following:

## Authors

Duane C. Pozza  
Partner  
202.719.4533  
dpozza@wiley.law

Joan Stewart  
Partner  
202.719.7438  
jstewart@wiley.law

Alissa Lynwood  
Associate  
202.719.4527  
alynwood@wiley.law

Melissa Alba  
Associate  
202.719.4729  
malba@wiley.law

## Practice Areas

FTC and Consumer Protection  
Privacy, Cyber & Data Governance  
State Privacy Laws  
Telecom, Media & Technology

- **Age Verification.** Developers must be able to (1) receive age category information from an app store, and (2) use this information to verify the age category of the app user. Under these laws, app stores must use commercially reasonable methods to verify a user's age upon account creation and share both age category and parental consent status with developers. While all three states require age verification, the specifics around the methods of verification are not fully harmonized.
- **Parental Consent.** If the app user is a minor, developers must be able to (1) receive parental consent information provided by the app store, and (2) use that information to verify whether a minor user is permitted to access the app or specific features, such as in-app purchases, before the app is downloaded or an in-app purchase is initiated. Developers must provide app stores with notice when there are significant changes to app terms, privacy policies, or monetization features. Parental consent must be refreshed after a significant change to the app or the policies that govern the app.
- **Age Rating.** Under the Texas law, developers have an explicit upstream obligation to (1) assign each app and each in-app purchase an age rating based on the law's defined age categories (i.e., <13, 13-15, 16-17, and 18+), and (2) provide that rating to each relevant app store.
- **Data Handling and Minimization.** Developers must also ensure that the information received from app stores for age verification and consent is only used for compliance purposes, transmitted securely using industry-standard encryption, and deleted after use (in Texas).

### Enforcement and Liability Landscape

The enforcement mechanisms established by the ASAAs introduce varying degrees of liability for developers and app store operators across the three states.

**Private Right of Action (PRA):** The ability for individuals to sue platforms directly varies between the states. Utah's law includes an explicit PRA, exposing developers to potential lawsuits for certain violations. The Texas law defines a violation as a "deceptive trade practice," which raises the possibility of private litigation.

**Government Enforcement:** In all three jurisdictions, violations can be pursued by the State Attorney General and carry the risk of substantial civil penalties.

**Safe Harbor Protection:** Texas and Utah grant developers a safe harbor based on reasonable reliance on information provided by an app store. However, Louisiana's law explicitly rejects this kind of safe harbor for developers.

### Compliance Approaches for Developers

Due to differences among the laws, developers cannot assume that legal requirements under ASAA laws are consistent across jurisdictions. Development and compliance teams must develop a full understanding of the nuances of each law and be aware of outlier requirements. Some key steps that developers should consider include:

- Preparing to receive and process age category and parental consent information from app stores;
- Reviewing app content and features to identify an appropriate age category for an app's intended audience, and determine if certain apps or features should be restricted for certain age levels;
- Considering the additional compliance obligations that may be triggered by receiving notice that an individual under the age of 13 is using the app (e.g., privacy obligations under the Children's Online Privacy Protection Act, or COPPA);
- Implementing a system to flag "significant changes" to Terms of Service or Privacy Policies and establishing a system to notify app stores; and
- Building out a method to track age verification and parental consent to provide clear records of compliance.

## Conclusion

In addition to these three laws, ASAA laws continue to be proposed and adopted. While these three laws are set to take effect in the coming months, several other state legislatures are considering similar laws, and California's Governor recently signed a law that functions somewhat differently but still involves collection and processing of age-related information. App developers should remain on top of these fast-changing requirements, and take proactive compliance steps that can be flexibly adapted to new requirements and shield against potential enforcement.

\*\*\*

Wiley's Privacy, Cyber & Data Governance team has broad experience in navigating compliance issues around cutting-edge technology and the evolving legal landscape, and handling enforcement and litigation matters. For questions about this alert, please contact the authors.