Tech Companies to Face New Safety Scrutiny: How Businesses Can Navigate the Upcoming Texas App Store Accountability Act

Insights
11.21.25

A new law about to take effect in Texas will force any company that either distributes software applications or develops apps to jump through safety-related hoops in an effort to protect minors. As of January 1, 2026, the App Store Accountability Act (ASAA) will force broadly defined "app stores" to verify every user's age, link minor accounts to a verified parent, and collect parental consent for each app download and in-app purchase. It will also push software developers to publish age ratings and honor those consent signals. Importantly the ASAA defines "app store" and "app developer" broadly to mean any company that distributes software applications and app developers that make their app available to any customer in Texas – even if not based in the state. While the law is already drawing constitutional challenges, you shouldn't rely on these challenges to prevent or delay compliance action to meet these new requirements. What do you need to know about this new law and what steps should you take to prepare for January 1?

What "App Store" Owners Need to Know

App store owners are the first defense to determine a user's age. Under the new law, they must use commercially reasonable methods of verification to verify the individual's age. They must also categorize the ages as under 13, 13-15, 16-17, and 18 and older.

Interestingly, the ASAA does not define commercially reasonable methods. However, another Texas statute lays out the following for reasonable age verification:

- the provision of digital identification, or
- compliance with a commercial age verification system that verifies age using government-issued identification, or a commercially reasonable method that relies on public or private transactional data to verify the age of an individual.

If the app store determines that an individual is under 18, the app store must:

- verify the identity of the adult affiliated with the minor's account and that the adult has the legal authority to make decisions on behalf of the minor, and
- obtain consent from the adult before the minor can download or purchase from the app store.

App stores must also limit the collection of personal data and must encrypt data during transmission. Further, app store owners must allow developers to access the age category and consent status of each user.

What App Developers Need to Know

Developers must assign their app with an age rating and identify the content that drives the rating. Additionally, before making significant changes to the software, developers must notify the app store. A significant change is something related to the personal data collection, changes to the age category, changes to the in-app purchases, and new advertisements in the app.

Developers also need a method to verify the age category of each user and whether consent has been obtained and they may only use personal data to enforce restrictions related to age and ensure compliance.

App developers will not be considered to be in violation of those specific aspects of the statute so long as they utilize industry standards to determine the age rating and apply those in good faith, as well as rely on the information received from the app store in good faith.

Enforcement

Importantly, the ASAA has a private right of action and a violation of the ASAA is considered a deceptive trade practice. That means that individuals who believe your company has violated the law will be able to file private lawsuits in court. Therefore, it is imperative that your organization take steps to prepare before January 1.

Your Action Plan

- Your organization should build a single, streamlined process for age verification and parental consent – as additional states will likely enact similar laws. In fact, Utah and Louisiana have already passed similar laws, and California's law will be effective in 2027.
- You should also update your privacy notices and app-store profiles to emphasize safety-by-design principles.
- Finally, you should inventory your apps and in-app purchases, assign and display ratings, and ensure that the store's age and consent signals are properly recognized. If these signals are missing or incomplete, you should block access until you can obtain proper verification.

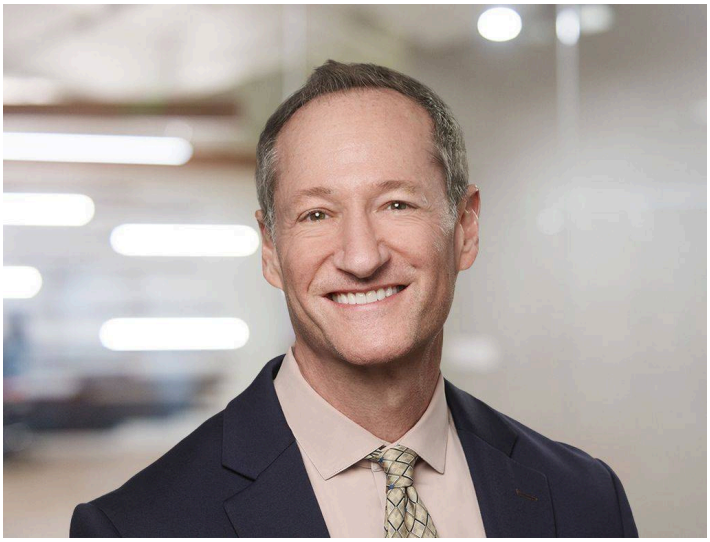
Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors

of this Insight, any member of our Data Protection and Cybersecurity Team, or any attorney in our Dallas or Houston offices.

Related People

Amanda E. Brown
Partner
214.220.8336
Email



Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

Jillian Seifrit, CIPP/US
Associate
610.230.6129
Email

Service Focus

Privacy and Cyber

Data Protection and Cybersecurity

Industry Focus

Tech

Related Offices

Dallas

Houston