

App Store Accountability Act

FREQUENTLY ASKED QUESTIONS



1. What are the key components of the App Store Accountability Act?

The App Store Accountability Act (ASAA) introduces key measures to protect children and restore parental authority in digital spaces:

App Store Age Verification: App stores must securely share verified age categories with apps, enabling developers to comply with laws like (Children’s Online Privacy Protection Act) COPPA and provide in-app experiences consistent with their stated age ratings, enhancing safety and simplifying compliance.

Accurate and Transparent Age Ratings: App age ratings must reflect actual content and in-app experiences, addressing the widespread concerns that apps misrepresent their suitability for children by downplaying mature content or features. It empowers parents to take legal action against misrepresented ratings and ensures accountability, transparency, and safer experiences for kids.

Mandatory Parental Consent: App stores must obtain verifiable parental consent before minors can download apps or make in-app purchases, protecting children from privacy risks, financial harm, and unenforceable contracts.

By closing loopholes and holding app stores accountable, the ASAA ensures platforms meet legal obligations, safeguard children’s rights, and create a safer digital space for families.

2. Why is the App Store Accountability Act Needed?

The App Store Accountability Act (ASAA) protects children online and restores parental control over digital spaces. Under contract law, minors cannot legally enter binding agreements without parental consent. Yet, app stores routinely allow known minors to download apps, accept terms of service, and make in-app purchases—often without any parental supervision. This loophole exposes children to privacy risks, financial harm, and dangerous digital environments, while app stores profit from a system that prioritizes revenue over families’ rights.

Recent investigations have exposed widespread misrating of apps as safe for children. Misleading age ratings, such as “12+,” give parents a false sense of security, leading them to trust apps that fail to protect their children. Some apps offer COPPA-compliant privacy protections and safer default settings for younger users, but these safeguards are often removed when children falsely claim to be older, leaving them exposed to significant privacy and safety risks.

When app stores fail to share a user’s verified age with apps, they actively mislead parents by advertising a safer experience while allowing apps to deliver variable and often inappropriate experiences once downloaded. This deliberate oversight frequently violates child protection laws, including COPPA, as app stores knowingly permit underage children to download restricted apps like social media. Inaccurate age ratings also render parental controls ineffective, as they depend on accurate and reliable age ratings to function properly.

App stores have already demonstrated their ability to securely and privately share age data through tools like “Verify for Wallet.” This shows that practical, effective solutions to protect children are not only feasible but well within reach.

3. How can we hold app stores accountable for protecting kids without complicating user experience?

The App Store Accountability Act (ASAA) provides an efficient framework for age verification and parental consent. By using app stores as centralized hubs, the ASAA could potentially leverage existing systems, such as Apple's Family Sharing and Google's Family Link, which already collect age and parental relationship data. This integration ensures compliance without creating additional burdens for users.

The ASAA has garnered support from leading child safety organizations, including the National Center on Sexual Exploitation and the Institute for Family Studies, as well as major tech companies like Meta. Renowned researcher Jonathan Haidt endorsed device-level age verification in *The Anxious Generation* as a critical step in creating safer online spaces for children.

Recent legal precedents support holding platforms liable for knowingly enabling harmful activities. The ASAA builds on this by requiring app stores to ensure compliance with child protection laws like (Children's Online Privacy Protection Act) COPPA and address misleading age ratings. These measures strengthen parental controls, empower parents to make informed decisions, and help protect children. By adhering to established legal principles and minimizing user disruption, the ASAA balances operational practicality with the pressing need to safeguard children in digital spaces.

4. Does this bill restrict free speech?

No, this bill focuses on ensuring legal compliance and enforcing parental consent for minors entering contracts, specifically in app distribution, not speech. It aligns with existing consumer protection regimes requiring parental consent for minors to agree to Terms of Service (TOS). It ensures age verification to obtain proper parental approval before minors enter binding agreements.

The bill also requires app stores to provide anonymized age data, helping developers comply with child protection laws like (Children's Online Privacy Protection Act) COPPA and ensuring minors do not enter unenforceable contracts. Additionally, the bill mandates accurate age ratings, addressing misleading or overly broad ratings that confuse parents and undermine the effectiveness of parental controls. By requiring accurate ratings, the bill empowers parents to make informed decisions and strengthens app store accountability.

App stores like Apple and Google already collect age data and have the ability to share it securely. Their failure to do so undermines child protection efforts. Rather than restricting speech, this bill ensures app stores meet their legal obligations to protect children and enforce parental consent.

5. How could app stores verify users' ages?

App stores could verify adult users by requiring them to link a credit card to their digital wallet, a feature already widely accessible and commonly used by nearly all app store users. This method is seamless and practical, as most adults already rely on credit cards for app and in-app purchases. Alternatively, app stores could adopt any of the numerous commercially available age verification systems to ensure compliance.

For children, app stores could require accounts for users under 18 to link to a verified adult supervisory account. During account setup, users already input their date of birth, and a parent or guardian could affirm this information to establish oversight.

To improve accuracy, app stores could leverage data already collected under existing privacy policies, such as device usage patterns or purchase history, to validate users' age information. By utilizing data that is typically already available, app stores can establish a secure, practical, and user-friendly framework for age verification, enhancing trust and privacy while prioritizing user safety.

6. How could app stores verify parental relationships?

App stores could handle verifying a parental relationship by requiring users under 18 to link their accounts to a verified adult supervisory account. Existing systems, such as Apple's Family Sharing and Google's Family Link, offer mechanisms to verify adult status securely by using the account holder's Apple ID or Google account, both tied to the adult's identity. Apple requires the family organizer to use their Apple ID and have a valid payment method, while Google relies on the adult's Google account and a payment method for purchase management.

These systems use multi-step setup processes designed to make it likely that only legitimate parents or guardians complete the linking. Secure methods, such as credit card authentication, add an additional layer of verification. App stores could further enhance this process with measures like cross-referencing shared last names on payment methods, using location data to confirm proximity between devices, or requiring parents or guardians to formally attest to the relationship.

7. Does the App Store Accountability Act conflict with the Children's Online Privacy Protection Act (COPPA)?

No, the App Store Accountability Act complements COPPA rather than conflicting with it. COPPA requires parental consent for collecting data from children under 13 but does not address the issue of minors entering agreements, such as terms of service or in-app purchases.

Under long-standing contract law, minors lack the capacity to enter binding agreements. Despite this, app stores routinely allow minors to enter such agreements without parental consent, disregarding both legal principles and parental authority. The App Store Accountability Act closes loopholes and weak enforcement mechanisms that have allowed app stores to bypass legal protections for minors and undermine parental rights.

9. Does the App Store Accountability Act create a burden on small developers?

The App Store Accountability Act places the primary responsibility for age verification and parental consent on app stores, the Act leverages existing infrastructure, allowing developers to focus on creating quality content without the need to build complex compliance systems.

This approach ensures that small developers meet legal requirements without significant additional costs or technical challenges. It promotes a safer online environment for children while supporting innovation and growth within the developer community.

10. Won't minors be able to circumvent age verification by using the browser version of an app?

In states with laws requiring age verification and/or parental consent for online platforms, users must provide this information to access the platform regardless of whether they use an app or a web browser.

Some platforms, like Snapchat, recognize the enhanced security of app stores and redirect users to the app store for first-time sign-ups. This ensures that age verification and parental consent requirements are handled effectively through the app store's processes.

Additionally, parents can use device-level parental controls to block or restrict web browsers, providing an added layer of protection. These tools help parents supervise their children's digital activities and reduce the risk of accessing platforms that may not enforce age verification as robustly as app stores.

Restores Parental Authority

Under long-standing contract law, minors cannot legally enter binding agreements without parental approval. The bill ensures that app stores verify parental consent before minors can download apps, agree to terms of service, or make in-app purchases.

Closes Dangerous Loopholes

App stores currently allow minors to bypass safeguards and enter agreements without parental consent. This exposes children to inappropriate content, privacy risks, and financial harm while platforms profit from invalid agreements.

Creates Accountability for Misleading Age Ratings

The bill empowers parents to hold app stores and developers accountable when apps misrepresent age ratings or content. By creating a private right of action, it incentivizes accurate ratings and safer app experiences for kids.

Requires App Stores to Share Anonymized Age Data

Many apps offer a range of in-app experiences based on user age. The bill requires app stores to securely share anonymized age data with developers so they can provide age-appropriate content and comply with child protection laws.

App Stores Already Have the Tools

App stores like Apple and Google already collect age and parental relationship data and use privacy-preserving tools, such as “Verify with Wallet.” The bill simply requires them to use these capabilities to protect children.

Streamlines Compliance for Developers

Small developers are not burdened. The bill places the responsibility for age verification on app stores, ensuring developers receive the information they need to comply without building complex new systems.

Balances Safety and Privacy

The bill protects user privacy while enabling stronger safeguards for children by sharing only anonymized age data. This approach builds on existing infrastructure without introducing unnecessary risks.

Targets App Stores' Conduct, Not Free Speech

The bill addresses app distribution practices, not content regulation. It ensures platforms comply with legal obligations, like verifying parental consent, without restricting free speech.