The App Store Accountability Act Would Undermine Privacy and Parental Choice

The App Store Accountability Act would require major app platforms to verify the ages of all users and restrict access for those under 18 without verified parental consent. While framed as a child protection measure, the bill would force app stores to collect sensitive personal data like government IDs or biometric scans from potentially hundreds of millions of users, posing serious risks to privacy, threatening free expression, and replicating the same constitutional flaws that have plagued previous online age-verification laws.

Mandatory age verification undermines privacy and security

- The bill would require platforms to collect sensitive personal data, like government-issued IDs or biometric scans, before users can access apps.
- This creates honeypots for hackers and significantly increases the risk of identity theft and surveillance.
- California's Age-Appropriate Design Code Act (CAADCA) introduced similar requirements. A federal judge blocked it, finding CAADCA "induces companies to collect additional personal information," increasing rather than reducing risk.
- Apple, Google, and potentially others would be forced to collect and store biometric templates or ID scans for every user, rolling back years of privacy gains.

It threatens free speech and limits access to information

- App stores aren't just for entertainment—they're how people access civic tools, education, and independent journalism. Forcing ID checks to reach that content raises clear First Amendment concerns.
- Courts have repeatedly struck down similar mandates. In *Reno v. ACLU* and *Ashcroft v. ACLU*, the Supreme Court made clear that age-gating access to legal speech is unconstitutional.
- The bill attempts to bypass those rulings by targeting app stores instead of social media platforms. But as the Court ruled in *Rutan v. Republican Party of Illinois*, what the government can't do directly, it also can't do indirectly.
- As *Packingham v. North Carolina* affirmed, "cyberspace" is now the most important forum for speech, and app stores are its front doors. Regulating that access point threatens core free speech rights.

Reason Foundation Technology Policy Contacts
Nicole Shekhovtsova, Policy Analyst (nicole.shekhovtsova@reason.org)
Marc Scribner, Senior Policy Analyst (marc.scribner@reason.org)

The government can't replace real parental involvement, but it creates a false sense of safety

- Most online age-verification regimes assume parents want rigid digital barriers—but research shows that many underage users access social media with parental knowledge or help.
- Legal mandates create a false sense of security, shifting responsibility from families to tech firms that cannot realistically enforce behavior within homes.
- Industry-led models like ESRB and MPAA ratings work because they empower—not override—parental discretion, offering guidance without coercion.
- A mandated age gate won't stop kids from using VPNs, browsers, or sideloaded apps—it will just make parents think the problem is solved.
- That false sense of safety undermines genuine efforts to educate kids, build digital literacy, and strengthen family-level boundaries.

Industry-led tools already help parents protect their kids online

- For example, Apple's parental control tools include Screen Time, Ask to Buy, content filters, communication limits, and age-based app restrictions.
- Child accounts come with default safety settings and allow parents to block downloads, limit content, and customize age settings.
- Current practices include: No personalized ads for users under 13, no cross-app tracking, and no forced identity collection.
- The Declared Age Range API lets developers serve age-appropriate content without collecting birthdates or IDs—a privacy-enhancing alternative to state-mandated verification.
- App stores already keep platforms safe from scams and malware precisely because they don't require sensitive personal data. Mandating age verification would undermine that balance and introduce new security risks.

It punishes small developers by adding compliance costs they can't afford

- Developers could be held liable if minors access their apps without proper age checks, exposing them to legal risk and forcing them to contract with costly third-party age-verification vendors.
- For small app developers operating on thin margins, even minor compliance friction (like age-gating pop-ups or verification screens) can be fatal. Adding age-verification and ID checks will lead to significant user drop-off. A Google study found just a one-second delay increases bounce rates by 32%, and three seconds by 53%.

Bottom line: The App Store Accountability Act would make age restrictions online more invasive than in any other area of daily life—requiring ID checks not just for social media, but for everyday apps that families already manage responsibly. Instead of building a surveillance regime around app downloads, lawmakers should support market-driven tools that empower parents and preserve user privacy.

Reason Foundation Technology Policy Contacts
Nicole Shekhovtsova, Policy Analyst (nicole.shekhovtsova@reason.org)
Marc Scribner, Senior Policy Analyst (marc.scribner@reason.org)