



1411 K St. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

Testimony from:
Josh Withrow, Fellow, Tech & Innovation Policy, R Street Institute

Testimony in opposition to SB 180, “An Act to require age verification before an individual may access an application from an online application store.”

February 18, 2025

South Dakota Senate Judiciary Committee

Chairman Wheeler and members of the committee,

My name is Josh Withrow, and I am a resident fellow with the Technology and Innovation Policy team at the R Street Institute, which is a nonprofit, nonpartisan, public policy research organization. Our mission is to engage in policy research and outreach to promote free markets and limited, effective government in many areas, including the technology and innovation sector. This is why we have a strong interest in Senate Bill 180.

We are concerned that SB 180, while in pursuit of the worthy goal of protecting minors from exposure to harmful content online, imposes an age-verification mandate that unduly burdens every consumer’s access to legal content and compromises the security and privacy of consumers’ data.¹ In return for these serious trade-offs, parents will receive less actual protection for minors than from existing tools which they can easily access and use on their own.²

SB 180 requires that any app store on a smartphone or internet-connected tablet device must verify a user’s age when creating an account. If the user’s age is determined to be under 18, the app store must then obtain “verifiable parental consent” before the minor can download or purchase any “covered application” – which as defined means effectively all apps – or make any in-app purchase. The bill then creates a broad private right of action under which any parent can sue the app store owners directly.³

In order to comply, app store owners will feel compelled to enact strict age verification for every device owner, whether via biometric scans or documentation.⁴ Even if the app stores are allowed to use a relatively anonymized age estimation technology, error rates for these technologies are high and some users will find themselves still having to provide further identification.⁵ Verifying parental status will necessarily be more even intrusive, likely requiring some sort of documentary identification like



1411 K St. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

government ID. Asking companies to determine parental consent is also difficult in practice because parents do not always share a last name with their dependent children, or a child's legal guardian may not be their actual parent at all.

The additional data that app stores will have to collect from consumers in order to comply with SB 180 also creates serious data security and privacy concerns. As if to emphasize this point, one of the biggest services used by some large social media platforms to verify user age and identity recently suffered a major data breach.⁶

SB 180's mandates are also redundant with existing protections already built into the major app stores. Apple's App Store and the Google Play store both have easily-used settings that parents can set to limit what apps and purchases their kids can access without their permission.⁷ Both also employ an app age-rating system similar to that for video games, so that parents can easily bar minors from downloading apps with a "T" or "M" rating, which would block all of the major social media and dating apps. There is also a thriving market for easy-to-use third-party software that parents can employ to lock down and monitor their kids' internet use on computers and smart devices that provide far more thorough protection than age-gating the app stores would ever provide.⁸

The ready availability of these alternative means to protect kids from online harms makes it very likely that this bill, such as other broad mandates to age-restrict access to general-use platforms, will be found unconstitutional. Previous attempts to enact broad age-gating restrictions for online services have been found to violate the First Amendment in the past. In the 1990s, the majority of the Communications Decency Act was struck down, with the U.S. Supreme Court finding unanimously that the law's "burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the Act's legitimate purposes."⁹

Similarly, requiring parental consent for minors to access lawful, non-obscene content was found to be unconstitutional, in *Brown v. Entertainment Merchants' Association*. Justice Antonin Scalia wrote in the majority, that "we note our doubts that punishing third parties for conveying protected speech to children just in case their parents disapprove of that speech is a proper governmental means of aiding parental authority."¹⁰



1411 K St. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

The privacy and cybersecurity concerns that are inherent in requiring the app stores to collect more personal data in order to verify users' age and parental status are also likely to tie this legislation up in court. A U.S. District Court decision in California placing an injunction on the state's Age Appropriate Design Code, found that the law was "actually likely to exacerbate the problem by inducing covered businesses to require consumers, including children, to divulge additional personal information."¹¹

Finally, even if the bill were to be held fully constitutional, its protections are easy for minors to work around. Apps dedicated to adult content are not allowed in the major app stores, for example, but violent and obscene content can easily be accessed via a mobile device's browser. Ultimately, there is no one-size-fits-all legislative solution that both protects minors from harmful content and interactions online and respects individual users' privacy and freedom of access to online content and speech.

We believe that lawmakers would be better off focusing on ways to improve online literacy, both for parents and their children, and encouraging parents to exercise the substantial power they already have to control what content and interactions their kids can access online. For all of these reasons, we respectfully oppose SB 180.

Thank you for your time and consideration,

Josh Withrow

Fellow, Technology & Innovation Policy
R Street Institute
(540) 604-3871
jwithrow@rstreet.org

¹ For a broad overview of problems with app store age verification proposals, see: Shoshana Weissmann and Josh Withrow, "No, conscripting the app stores doesn't solve the problems with age verification," *R Street Institute*, Jan 29, 2025. <https://www.rstreet.org/commentary/no-conscripting-the-app-stores-doesnt-solve-the-problems-with-age-verification/>.

² For example, a quick step-by-step walkthrough for how to enable existing parental controls on any commonly-owned mobile device: "Parental Controls," Internet Matters, <https://www.internetmatters.org/parental-controls/>.



1411 K St. NW
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

³ South Dakota Senate, 2025 Legislative Session, Senate Bill 180, Last accessed February 16, 2025:
<https://sdlegislature.gov/Session/Bill/26140>.

⁴ See Shoshana Weissmann, et al. “The Fundamental Problems with Social Media Age Verification Legislation,” *R Street Institute* May 16, 2023. <https://www.rstreet.org/commentary/the-fundamental-problems-with-social-media-age-verification-legislation/>.

⁵ On error rates for the best age verification technologies, see: Kayee Hanaoka, et al., “Face Analysis Technology Evaluation: Age Estimation and Verification,” *NIST Internal Report 8525*, May 2024.
<https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8525.pdf>.

⁶ Jason Kelley, “Hack of Age Verification Company Shows Privacy Danger of Social Media Laws,” *Electronic Frontier Foundation*, June 26, 2024. <https://www.eff.org/deeplinks/2024/06/hack-age-verification-company-shows-privacy-danger-social-media-laws>

⁷ “Approve what kids buy with Ask to Buy,” Last accessed Feb. 16, 2025. <https://support.apple.com/en-us/105055>, and “Purchase approvals on Google Play,” Last accessed Feb. 16, 2025.
<https://support.google.com/families/answer/7039872?hl=en&co=GENIE.Platform%3DAndroid>.

⁸ “Children Online Safety Tools,” *Competitive Enterprise Institute*, Last accessed Feb. 16, 2025.
<https://cei.org/children-online-safety-tools/>.

⁹ *Reno v. ACLU*, 521 U.S. 844 (1997), U.S. Supreme Court, June 26, 1997.
<https://supreme.justia.com/cases/federal/us/521/844>.

¹⁰ *Brown et al. v. Entertainment Merchants Assn. et al.*, 564 U.S. 786 (2011). U.S. Supreme Court, June 27, 2011.
<https://supreme.justia.com/cases/federal/us/564/786>.

¹¹ Adrian Moore and Eric Goldman, “California’s Online Age-Verification Law is Unconstitutional,” *Reason*, Nov. 28, 2023. <https://reason.org/commentary/californias-online-age-verification-law-is-unconstitutional/>.