AMERICAN CIVIL LIBERTIES UNION
Wisconsin

207 East Buffalo Street, Suite 325
Milwaukee, WI 53202
(414) 272-4032
aclu-wi.org

ACLU of Wisconsin Comments re: Assembly Bill 962

The ACLU of Wisconsin understands and shares the ultimate goal of protecting young people from harm and appreciates the opportunity to provide written comments highlighting the constitutional and practical concerns regarding this bill.

While AB-962 is intended to protect and support children and families online, this bill goes far beyond that goal. It would impose sweeping age verification and parental consent requirements that burden lawful speech, centralize sensitive personal data, and undermine the autonomy and development of older minors.

At its core, AB-962 deputizes app stores and app developers as gatekeepers of speech. By requiring age ratings, content descriptions, and the enforcement of age-based restrictions, the bill is not merely about contracts or consumer protection—it's about speech. A federal court in the Western District of Texas granted preliminary injunctions against Texas's recently enacted "App Store Accountability Act"[1] (which is strikingly similar to the text of AB-962), concluding that the law is a content-based statute subject to strict scrutiny and likely violates the First Amendment.[2] In the introduction to the court's orders, it described the Act as "akin to a law that would require every bookstore to verify the age of every customer at the door and, for minors, require parental consent before the child or teen could enter and again when they purchase a book."

AB-962 would require app store providers to collect and verify age category information for nearly all users—including existing users, and including adults—then assign them to rigid age-buckets that follow them across their devices and applications. Verifying a user's age category "using a commercially available method of age verification that is reasonably designed to ensure accuracy" could include uploading a driver's license or state ID, completing a biometric face scan that uses artificial intelligence to estimate an age, or using a credit card to estimate an age based on private transactional data. That age category data must then be shared with developers and repeatedly rechecked throughout the life of an app, including for pre-installed apps that come standard on a device. **This creates an operating-system-level gatekeeping system that reaches into nearly every aspect of a person's digital life.**

Even though the bill claims to limit data use and requires encryption, it still mandates the collection, verification, and long-term retention of age-related identity markers.

---

[1] S.B. 2420, https://capitol.texas.gov/tlodocs/89R/billtext/pdf/SB02420F.pdf.
[2] *Students Engaged in Advancing Texas, et al. v. Paxton*, No. 1:25-CV-1662-RP, 2025 WL 3731733 (W.D. Tex. Dec. 23, 2025), https://storage.courtlistener.com/recap/gov.uscourts.txwd.1172870103/gov.uscourts.txwd.1172870103.38.0.pdf; *Computer & Communications Industry Association v. Paxton,* No. 1:25-CV-1660-RP, 2025 WL 3731733 (W.D. Tex. Dec. 23, 2025), https://storage.courtlistener.com/recap/gov.uscourts.txwd.1172869998/gov.uscourts.txwd.1172869998.65.0.pdf.

Centralizing this information at the app store level concentrates enormous responsibility and risk in a small number of entities. Large platforms are frequent targets of data breaches, and no system is immune. **A breach involving age verification data would expose sensitive information about individual minors at massive scale, information that could be exploited for years to come.**

Once a user is designated a "minor," that status becomes a persistent identity marker. It follows them across apps. It is shared with developers. It triggers ongoing parental consent requirements for downloads, purchases, in-app purchases, and even continued use after a "significant change." **This structure assumes that parental involvement is always safe, appropriate, and beneficial. That assumption does not reflect reality.** These risks are particularly acute for LGBTQ+ youth, young people in unsupportive or abusive homes, and teens who rely on privacy, anonymity, or peer-to-peer support to explore questions of identity, sexual health, or personal safety.

AB-962 is also deeply flawed in how it treats older minors. **Under this bill, a 16- or 17-year-old high school student on the verge of adulthood is regulated in fundamentally the same way as a 13-year-old middle schooler.** Older teens are trusted to drive cars, work full-time jobs, and make decisions with real consequences for their safety and future. They could weeks or months away from voting, from moving across the country, and from being treated as full legal adults. **Yet under this bill, they are denied the ability to independently access apps or information without ongoing parental permission.**

This is not a neutral policy choice. It reflects a profound mistrust of young people at precisely the stage of life when developing independent thought, identity, and values is most critical. The ability to seek out information, culture, and community separately from one's parents is not a threat to society. It is how societies grow, adapt, and improve. **Imagine if throughout American history, young people—who have always been at the forefront of change—were denied access to ideas their parents opposed.** Cultural and democratic progress depends on young people being able to encounter new ideas and form their own beliefs. That process should not be stifled by law.

As Justice Scalia noted for the majority in a decision striking down a California law requiring parental consent for minors to access lawful, non-obscene content, "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."[3]

[3] *Brown v. Entertainment Merchants Ass'n*, 564 U.S. 786, 802 (2011).