January 28, 2026

Senate Judiciary Committee
300 SW 10th St
Topeka, KS 66612

Re: SB 372 – App Store Accountability Act (Oppose)

Dear Chair Warren and Members of the Senate Judiciary Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 372 in advance of the Committee hearing on January 28, 2026. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members.

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and parental tools to individually tailor younger users' online use to their developmental needs. For example, various services allow parents to set time limits, provide enhanced privacy protections by default for known child users, and other tools allow parents to block specific sites entirely.[2] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.

SB 372 raises many concerns including proposed age verification and parental consent requirements for covered app store providers and developers. The bill risks subjecting businesses to vague compliance requirements and arbitrary enforcement, while jeopardizing consumer privacy. We appreciate the opportunity to elaborate on these concerns as the Committee considers this proposal.

Courts have repeatedly struck down laws containing speech restrictions intended to prevent harm to minors.

In 1997, the Supreme Court held that "the First Amendment does not tolerate" laws that "reduce[] the adult population … to reading only what is fit for children."[3] Yet SB 372 effectively does exactly this: in order to restrict access to content potentially harmful to children, the proposed bill would restrict both children and adults' access to such content. The First Amendment applies to teens as well as adults.[4]

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.
[2] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated June 10, 2025).
[3] *Reno v. ACLU*, 521 U.S. 844, 888 (1997) (cleaned up).
[4] *See, e.g.*, *id.* at 855-56.

Nor do states have the authority to require parental consent for viewing such content; the Court has likewise rejected the argument that "the state has the power to prevent children from hearing or saying anything without their parents' prior consent."[5] Accordingly, the proposed bill unconstitutionally undermines established free speech protections for users of all ages.

For these reasons, the vast majority of lower courts that have ruled on the issue have held that the First Amendment does not permit states to require age verification to access protected speech.[6] Most recently, a Texas federal court recently blocked a similar mandate on First Amendment grounds, noting that since "nothing suggests Texas's interest in preventing minors from accessing a wide variety of apps that foster protected speech (such as the Associated Press, the Wall Street Journal, Substack, or Sports Illustrated) is compelling,"[7] such a law "fails strict scrutiny" and "would fail intermediate scrutiny as well."[8]

Age verification and parental consent requirements undermine user privacy for users of all ages.

SB 372's requirements undermine privacy for all users. While well-meaning, age verification mandates inherently require collecting sensitive data about users and adults. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[9] Requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.[10]

Such dangers are far from hypothetical: Several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[11] Furthermore, government officials could access this sensitive data through enforcement inquiries and processes. Compounding these problems, the bill requires covered online services to retroactively verify the ages of existing users as well as prospective ones, which unnecessarily increases the risk of malicious actors accessing the data submitted.

---

[5] *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 795 n. 3 (2011).
[6] *See, e.g.*, *CCIA v. Paxton*, No. 25-cv-01660, 2025 WL 3754045 (W.D. Tex. Dec. 23, 2025); *SEAT v. Paxton*, No. 25-cv-01662, 2025 WL 3731733 (W.D. Tex. Dec. 23, 2025); *NetChoice v. Griffin*, No. 5:25-CV-5140 (W.D. Ark. Dec. 15, 2025); *NetChoice v. Murrill*, No. 25-231, 2025 WL 3634112 (M.D. La. Dec. 15, 2025); *NetChoice v. Carr*, 789 F. Supp. 3d 1200 (N.D. Ga. 2025); *NetChoice v. Yost*, 778 F. Supp. 3d 923 (S.D. Ohio 2025); *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 (W.D. Ark. Mar. 31, 2025); *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024); *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024).
[7] *NetChoice v. Paxton*, 2025 WL 3754045 at *12; *SEAT v. Paxton*,2025 WL 3731733 at *11.
[8] *NetChoice v. Paxton*, 2025 WL 3754045 at *14-15; *SEAT v. Paxton*, 2025 WL 3731733 at *14.
[9] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *Principle (c): Data Minimisation,* U.K. Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.
[10] Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, R St. Inst. (May 24, 2023), https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/.
[11] *See, e.g.*, Mark Tsagas, *Online Age Checking Is Creating a Treasure Trove of Data for Hackers*, The Conversation (Nov. 11, 2025), https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586.

The more data a service is forced to collect, the greater risk it poses to consumer privacy and small business sustainability.[12] A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification methods, and that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[13]

The Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.[14] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

Additionally, the data access requirement would undermine privacy and make children less safe, as developers would be forced to collect sensitive personal information identifying an app store provider's users, including parents of their underage customers.

Moreover, the bill undermines user privacy without impacting younger users' ability to access most of the apps in question. Verifying age only for operating system and application store users overlooks access to websites via other means. Numerous applications are designed for web browsers, which this method does not cover. While application store age verification might seem like a comprehensive bulwark against certain content deemed undesirable for younger users, in reality, it falls short of achieving that goal.

The private right of action would result in the proliferation of frivolous lawsuits and questionable claims, and exorbitant statutory damages.

SB 372 permits users to bring legal action against persons that have been accused of violating new regulations. The bill would enable a "minor, or the parent or guardian of the minor, who has been harmed by a violation" to "bring a civil action against an app store provider or a developer" for "the greater of actual damages or $1,000 for each violation," as well as "punitive damages if the violation was egregious" and "reasonable attorney fees and costs." By creating a new private right of action, the measure would open the doors of Kansas's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. As lawsuits prove extremely costly and time-intensive, it is foreseeable that these costs would be passed on to individuals in Kansas, disproportionately impacting smaller businesses and startups across the state.

* * * * *

[12] Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Aug. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.
[13] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023) at 10, https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[14] *Online Age Verification: Balancing Privacy and the Protection of Minors,* CNIL (Sept. 22, 2022), https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Respectfully submitted,

Megan Stokes
Director of State Policy
Computer & Communications Industry Association