March 31, 2025

Texas Senate
Attn: Senate State Affairs Committee
1100 Congress Ave
Austin, Texas 78701

Re: SB 2420 – "Relating to the regulation of platforms for the sale and distribution of software applications for mobile devices." (Oppose)

Dear Chair Hughes and Members of the Senate State Affairs Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 2420. 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.[3]

The proposed age verification and parental consent requirements for covered application store providers and developers raise significant concerns. The bill risks subjecting businesses to vague compliance requirements and arbitrary enforcement, while jeopardizing consumer privacy. We appreciate the opportunity to expand on these concerns as the Committee considers this proposal.

Requirements under SB 2420 are not administrable or well defined, creating serious compliance questions for businesses and users.

SB 2420 contains vague definitions that do not allow covered entities to know if they are complying with the law. The bill requires that app stores use "reasonable means" to notify parents, and "use a commercially reasonable method" of age verification. The bill does not define these terms further, placing any covered entity serving minors in legal uncertainty.

---

[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 Feb. 19, 2025).
[3] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.

Rather than protect minors online, such vague language incentivizes companies to stop serving these populations entirely.

Furthermore, age verification bills carry inherent compliance difficulties. Requiring companies to collect more user data even as other states require collecting less data places businesses in the untenable position of picking which state laws to comply with, and which to unintentionally violate.[4] Additionally, verifying age only for 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.

To avoid restricting teens' access to information, SB 2420 should regulate users under 13 rather than 18 in accordance with established practices.

SB 2420 defines a "minor" as "a child who is younger than 18 years of age who has not had the disabilities of minority removed for general purposes." We would suggest changing the definition of "minor" to a user under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard. This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources.

Currently available tools to conduct age determination are imperfect in estimating users' ages.

Every approach to age determination presents trade-offs between accuracy and privacy[5]—in addition to significant costs, especially for startups[6]—and there is no one-size-fits-all approach. Different services consider various factors, including but not limited to their user base, the service offered, risk calculation, privacy expectations, and economic feasibility. A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains guiding principles for age assurance and discusses how digital services have used such principles to develop best practices.[7]

The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[8] The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA

[4] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard.
[5] Kate Ruane, *CDT Files Brief in Netchoice v. Bonta Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[6] Engine, *More than just a number: How determining user age impacts startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d51f0b0d4f007b71fe2ba6/1708465932202/Engine+Report+-+More+Than+Just+A+Number.pdf.
[7] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[8] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* National Institute of Standards & Technology (May 30, 2024), https://doi.org/10.6028/NIST.IR.8525.

encourages lawmakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

Age verification and parental consent requirements raise significant privacy concerns.

Every approach to age determination presents trade-offs between accuracy and privacy[9]—in addition to significant costs, especially for startups[10]—and there is no one-size-fits-all approach. Different services consider various factors, including but not limited to their user base, the service offered, risk calculation, privacy expectations, and economic feasibility. A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains guiding principles for age assurance and discusses how digital services have used such principles to develop best practices.[11]

The proposed bill suggests imposing a government-mandated requirement to verify all Texas users' ages that conflicts with data minimization principles ingrained in standard federal and international privacy and data protection compliance practices.[12] Determining a user's age and verifying parental consent inherently requires collecting additional sensitive data from those users, and any document capable of verifying a user's age will likely contain sensitive information. Such excessive monitoring has been shown to negatively affect young people's mental health and development.[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.

---

[9] Kate Ruane, *CDT Files Brief in NetChoice v. Bonta Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[10] Engine, *More than just a number: How determining user age impacts startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d51f0b0d4f007b71fe2ba6/1708465932202/Engine+Report+-+More+Than+Just+A+Number.pdf.
[11] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[12] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *see also 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/.
[13] *See, e.g.*, Hannah Quay-de la Valle, *The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks*, Ctr. for Democracy & Tech. (May 5, 2022), https://cdt.org/insights/the-chilling-effect-of-student-monitoring-disproportionate-impacts-and-mental-health-risks/ (finding that "Monitoring programs, if not carefully implemented, can stifle growth and leave students vulnerable to the chilling effect, placing their mental health at risk").
[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.

Age verification and parental consent requirements for online businesses are currently being litigated in several jurisdictions.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.[15] After 25 years, age authentication still remains a vexing technical and social challenge.[16]

Recent state legislation that would implement online parental consent and age verification or estimation measures is currently facing numerous constitutional challenges, and numerous federal judges have placed laws on hold until these challenges can be fully reviewed, including in Arkansas, California, Mississippi, Ohio, Tennessee, Texas, and Utah.[17] CCIA anticipates that forthcoming rulings from the judiciary may be instructive in determining how, or whether, age determination requirements can be tied to granting user access to online speech. CCIA therefore recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated and passing on expensive litigation costs to taxpayers.

* * * * *

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.

Sincerely,

Tom Mann
State Policy Manager, South
Computer & Communications Industry Association

[15] *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).
[16] Jackie Snow, *Why age verification is so difficult for websites*, Wall St. J. (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.
[17] *See, e.g.*, *NetChoice v. Bonta*, No. 24-cv-07885, 2025 WL 28610 (N.D. Cal. Jan. 2, 2025); *NetChoice v. Bonta*, No. 22-cv-08861, 2024 WL 5264045 (N.D. Cal. Dec. 31, 2024); *NetChoice, LLC v. Reyes*, No. 23-cv-00911, 2024 WL 4135626 (D. Utah Sept. 10, 2024); *NetChoice, LLC v. Fitch*, No. 24-cv-00170, 2024 WL 3276409 (S.D. Miss. July 1, 2024); *NetChoice, LLC v. Yost*, 716 F. Supp. 3d 539 (S.D. Ohio 2024); *NetChoice, LLC v. Griffin*, No. 23-cv-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023); *Comput. & Commc'ns Indus. Ass'n et al. v. Paxton*, No. 24-cv-00849, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024).