



February 14, 2025

Senate Judiciary Committee
South Dakota State Capitol
500 E Capitol Ave
Pierre, SD 57501

Re: SB 180 – "require age verification before an individual may access an application from an online application store." (Oppose)

Dear Chair Wheeler and Members of the Senate Judiciary Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 180 in advance of the Senate Judiciary Committee hearing on February 18, 2025. 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 180 are not administrable or well defined, creating serious compliance questions for both businesses and users and making minors less safe.

SB 180 contains vague definitions that would impose significant requirements and restrictions on application store providers and developers. The bill contains an overly broad knowledge standard that would hold covered entities liable for "knowledge fairly inferred based on

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/>.

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/>.

objective circumstances,” leaving businesses without any concrete guidelines as to when they might face liability. Sections 2(3) and 4(3) would also impose burdensome recurring notice and renewed consent requirements, including over any so-called “significant change” to an application’s terms of service or privacy policy. Such requirements apply whenever a modification “[m]aterially changes the functionality of the application or the application’s user experience,” with no objective criteria for businesses to know what constitutes a “material[] change.”

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

Every approach to age determination presents trade-offs between accuracy and privacy⁴—in addition to significant costs, especially for startups⁵—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.⁶

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.⁷ 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 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.

The proposed bill suggests imposing a government-mandated requirement to verify all South Dakota users’ ages that conflicts with data minimization principles ingrained in standard federal and international privacy and data protection compliance practices.⁸ 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. Requiring companies to collect more user data even as other states

⁴ 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/>.

⁵ 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>.

⁶ *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.

⁷ 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>.

⁸ 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/>.

require collecting less data places businesses in the untenable position of picking which state laws to comply with, and which to unintentionally violate.⁹

Additionally, 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 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.¹⁰ Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

Furthermore, Section 2(4)'s real-time data access requirement would undermine privacy and make children less safe, as developers would have access to sensitive personal information identifying an app store provider's users, including parents of their underage customers.

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.¹¹ After 25 years, age authentication still remains a vexing technical and social challenge.¹²

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.¹³ 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.

⁹ 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>.

¹⁰ *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>.

¹¹ *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).

¹² 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>.

¹³ 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).



Investing sole enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

SB 180 permits “the parent of a minor who has been harmed by a violation” to bring legal action against a provider. There is no guidance or restriction on how they may have allegedly been “harmed.” By creating a new private right of action, this measure allows plaintiffs to advance frivolous claims with little evidence of actual injury. Such lawsuits also prove extremely costly and time-intensive, with the costs being passed on to individual Washington consumers. Such a measure would disproportionately impact smaller businesses and startups across the state. Further, investing sole enforcement authority with the state attorney general allows for the leveraging of technical expertise concerning enforcement authority, and allows public interest to determine which enforcement actions are brought.

CCIA also recommends that the legislation include a cure period of at least 30 days. This would allow for actors operating in good faith to correct unknowing or technical violations, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. It would also focus the government’s limited resources on those that persist in knowingly violating the law. Such notice allows consumers to receive injunctive relief, but without the time and expense of bringing a formal suit. The proposed safe harbor for developers is appreciated, but insufficient.

* * * * *

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,

Megan Stokes
State Policy Director
Computer & Communications Industry Association