



January 8, 2026

New Jersey Senate Committee on Budget and Appropriations
State House Annex
Trenton, NJ 08608

Re: A. 4664 and S. 4153- An Act prohibiting social media platforms from promoting certain eating behaviors to child users and supplementing Title 56 of the Revised Statutes. (Oppose)

Dear Chair Sarlo, Vice Chair Greenstein, and Members of the Senate Committee on Budget and Appropriations:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose A. 4664 and S. 4153. 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

However, protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Lawful speech cannot be suppressed solely to protect young online users from ideas or images that a legislative body disfavors.³ While CCIA shares the goal of increasing online safety, these bills present the following concerns.

The Supreme Court has 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.”⁴ Yet A. 4664 and S. 4153 effectively do exactly this: in order to restrict access to content potentially harmful to children, the proposed bills would restrict both children and adults' access to such content.

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 *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212–14 (1975). See also *FCC v. Pacifica Found.* 438 U.S. 726, 749–50 (1978); *Pinkus v. United States*, 436 U.S. 293, 296–98 (1978).

⁴ *Reno v. ACLU*, 521 U.S. 844, 888 (1997) (cleaned up).

The First Amendment applies to teens as well as adults,⁵ and to content posted on social media.⁶

Moreover, the Court has held that “The First Amendment’s guarantee of free speech does not extend only to categories of speech that survive an ad hoc balancing of relative social costs and benefits”⁷ — states cannot restrict access to content even if harms might result from viewing it. Nor do states have the authority to require parental consent for such viewing; 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.”⁸ Accordingly, the proposed bills unconstitutionally undermine established free speech protections for users of all ages.

The bills do not specify how a user’s age is to be determined.

A. 4664 and S. 4153 would require covered services to treat users under the age of 18 (what the bills refer to as “child users”) differently from all other users. However, the bills fail to explain how each covered service would determine which of their users are under 18. Accordingly, the bills fail to determine which covered services have complied with age-specific prohibitions for a “design, algorithm, practice, affordance, or feature that the platform knows, or which by the exercise of reasonable care should have known, could cause child users to develop an eating disorder. . . .” Covered services will thus be unable to determine with certainty whether they are complying with the law.

The bills’ requirements undermine user privacy and competition.

There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy⁹ and small business sustainability.¹⁰ Because covered businesses’ legal obligations are so vaguely defined, they will effectively be forced to adopt age verification measures to minimize the risk of noncompliance. These bills therefore undermine privacy by effectively forcing covered businesses to overcollect sensitive data from both minors and adults.

Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.¹¹ 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.¹² Such dangers are far

⁵ See, e.g., *id.* at 855-56.

⁶ See, e.g., *Packingham v. North Carolina*, 582 U.S. 98, 105-06 (2017).

⁷ *United States v. Stevens*, 559 U.S. 460, 470 (2010).

⁸ *Brown v. Ent. Merchs. Ass’n*, 564 U.S. 786, 795 n. 3 (2011).

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* (Aug. 2024),

<https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+T+han+Just+A+Number+-+Updated+August+2024.pdf>.

¹¹ 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/>.

¹² Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don’t Intend That*, R St. Inst. (May 24, 2023),

from hypothetical: Several of the most devastating data breaches in recent years are directly attributable to age verification requirements.¹³

Moreover, forcing widespread adoption of age verification undermines competition. A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains more information regarding guiding principles for age assurance and how digital services have used such principles to develop best practices.¹⁴ The report found that “smaller companies may not be able to sustain their business” if forced to determine user ages, and that “[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID.”¹⁵

The bills lack clear definitions, which will result in legitimate speech being censored — especially given the \$250,000 statutory penalty.

Besides imposing vague legal obligations on covered businesses, the proposed bills contain several vague definitions which risk broadening their scope far beyond the likely intended focus. For instance, the term “diet products” is undefined in the bills and could reasonably be interpreted to include items like vitamins, nutritional supplements, as well as even exercise or workout videos, all of which young adults could reasonably want to access to promote healthy habits and lifestyle. (Is skim milk a “diet product”? Is medication for juvenile diabetes? Is a salad? What about the Heart Healthy soup line from New Jersey’s own Campbell’s?)

The combination of overly broad definitions and the lack of definitions for key terms would likely result in an over-moderation of content in order to avoid any risk of running afoul of the law — especially given the bills’ extreme \$250,000 statutory penalty. Further, because definitions are so broad or entirely lacking, the bills are likely to encompass various categories of unambiguously protected speech preventing users from accessing important resources and communities of support.

If enacted, these bills may result in denying services to all users under 18, limiting their access to needed supportive communities.

The lack of narrowly tailored definitions, as discussed above, could incentivize businesses to simply prohibit minors from using digital services rather than face potential legal action and hefty fines for non-compliance. Requiring businesses to deny access to social networking sites or other online resources may also unintentionally restrict children’s ability to access and connect with like-minded individuals and communities. For example, children of certain minority groups may not live in an area where they can easily connect with others that

<https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/>.

¹³ 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>.

¹⁴ *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.

¹⁵ *Id.* at 10.



represent and relate to their own unique experiences, so an online central meeting place where kids can share their experiences and find support can have positive impacts.¹⁶

The connected nature of social media has led some to allege that online services may be negatively impacting teenagers’ mental health. However, researchers explain that this theory is not well supported by existing evidence and repeats a ‘moral panic’ argument frequently associated with new technologies and modes of communication. Instead, social media effects are nuanced,¹⁷ individualized, reciprocal over time, and gender-specific.

As explained above, CCIA believes that an alternative to solving these complex issues is to work with businesses to continue their ongoing private efforts to implement mechanisms such as daily time limits or child-safe searching so that parents can have control over their own child’s social media use.

* * * * *

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

Respectfully submitted,

Kyle J. Sepe
State Policy Manager, Northeast Region
Computer & Communications Industry Association

¹⁶ *The Importance of Belonging: Developmental Context of Adolescence*, Boston Children’s Hospital Digital Wellness Lab (Oct. 2024), <https://digitalwellnesslab.org/research-briefs/young-peoples-sense-of-belonging-online/>.

¹⁷ Amy Orben et al., *Social Media’s Enduring Effect on Adolescent Life Satisfaction*, PNAS (May 6, 2019), <https://www.pnas.org/doi/10.1073/pnas.1902058116>.