



February 18, 2026

New Jersey Assembly Committee on Science, Innovation and Technology
Committee Room 13, 4th Floor, State House Annex
Trenton, NJ 08608

Re: A 4015 - “New Jersey Kids Code Act” (Oppose)

Dear Chair Tully, Vice Chair Singh, and Members of the Committee on Science, Innovation and Technology:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose A 4015. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.¹ Proposed regulations on the intrastate provision of digital services therefore can have a significant, nationwide impact on CCIA members.

CCIA firmly believes that children are entitled to security and privacy online. Our members have designed and developed 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, while CCIA shares the goal of increasing online safety for minors, A 4015 introduces significant constitutional, operational, and privacy concerns that would negatively impact New Jersey residents and businesses.

A 4015’s method of designating covered services violates the First and Fourteenth Amendments.

In 2024, the Supreme Court ruled that “regulating the content-moderation policies that the major platforms use for their feeds... to change the speech that will be displayed there... is a preference” that states “may not impose.”³ However, A 4015 requires “rules that prohibit or limit data processing practices or covered design features that facilitate compulsive use by covered minors or impair autonomy, decision making, or choice of covered minors.” “Covered design features” include “quantification of engagement, including, but not limited to, providing a visible count of how many likes, comments, clicks, views, or reactions a user-generated item has received”. Federal courts have found that restricting such displays violates the First Amendment.⁴ By broadly controlling how services organize, present, and prioritize information to users, the bill creates impermissible content-based restrictions on speech.

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 *Moody v. NetChoice*, 144 S. Ct. 2383, 2408 (2024).

⁴ See, e.g., *NetChoice v. Bonta*, 152 F.4th 1002, 1016-17 (9th Cir. 2025).



A 4015's findings inaccurately describe the research regarding minors and social media use.

Much research on social media and adolescent health (including the National Academies of Sciences, the University of Oxford, the American Psychological Association, and the Journal of Pediatrics) has found that social media does not cause changes in adolescent health at the population level.⁵ Even the Surgeon General's Social Media and Youth Mental Health advisory referenced in A 4015 acknowledges the benefits of social media, including social connection, information sharing, and civic engagement.⁶ Indeed, as a federal court recently noted, "nearly all of the research showing any harmful effects" for minors on social media "is based on correlation, not evidence of causation."⁷

The bill's requirements are not well-defined.

Most privacy laws that prohibit the use of "dark patterns" do so only in specific contexts, such as to obtain consent.⁸ A 4015, however, does not contextualize the prohibition on "dark patterns." Without such contextual information, prohibiting interface designs "with the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice" is a vague requirement. Deciding when design features impair *any* choice a consumer might make is far more subjective than determining when such features impair the choice to provide consent. This requirement should therefore be specific to the consent context.

The bill's scope is overly broad.

A 4015 covers any business who "annually processes the personal data of not less than 50,000 consumers or households..." This definition covers many small businesses, even those whose services are primarily offline (e.g., a theme park with a reservation portal, a clothing store that sells several items in children's sizes, etc.). Consequently, any such businesses with users under 18 would be subject to extensive compliance requirements, including ensuring that users can disable all design features (which in many cases may not be feasible). This vast array of businesses will also have to institute time limits, parental controls, purchase limits, and many other features requiring significant technical capabilities that many businesses may not possess. A coffee shop, for instance, might need to develop a method for parents to limit their children's ability to purchase a coffee, etc.

⁵ Regina Park, *The Internet Isn't Harmful to Your Mental Health, Oxford Study Finds*, Disruptive Competition Project (Jan. 29, 2024),

<https://project-disco.org/innovation/the-internet-isnt-harmful-to-your-mental-health-oxford-study-finds/>.

⁶ Mike Masnick, *Warning: Believing The Surgeon General's Social Media Warning May Be Hazardous To Teens' Health*, Techdirt (June 18, 2024),

<https://www.techdirt.com/2024/06/18/warning-believing-the-surgeon-generals-social-media-warning-may-be-hazardous-to-teens-health/>.

⁷ *NetChoice v. Yost*, No. 2:24-cv-00047, 2025 WL 1137485 at *21 (S.D. Ohio Apr. 16, 2025).

⁸ See, e.g., Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.001(6)(C) (West 2024),

<https://statutes.capitol.texas.gov/?tab=1&code=BC&chapter=BC.541&artSec=>; Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515(7)(C) (2024), https://www.cga.ct.gov/2024/sup/chap_743jj.htm.



The bill incentivizes overcollection of minors' data.

A 4015 also requires that covered businesses not “send a notification to a covered minor between 10 p.m. and 6 a.m. and, on a weekday between Labor Day and Memorial Day, between 8 a.m. and 4 p.m.” Such requirements inevitably require that covered operators track when it is nighttime in a given device’s location. This requirement therefore effectively mandates location-based tracking of minors’ devices, thus undermining the privacy of the very population the bill is designed to protect. Requiring covered operators to track their users serves no benefit, particularly since covered operators regularly offer users the option to turn off notifications themselves.

The bill requires audits without an appropriate framework in place.

Section 13 provides that a covered provider covered online service must issue a public report prepared by an independent third-party auditor that contains “a detailed description of the online service as pertaining to minors, including the online service’s covered design features, use of personal data, and business practices.” Formal audits, however, are intended to demonstrate compliance with detailed sets of specifications⁹ rather than general principles. Audits are not designed to evaluate subjective criteria such as whether a provider is “likely to be accessed by minors” or whether a given feature will “encourage or increase the frequency, time spent, or activity of a user on the online service.” No framework for evaluating such subjective criteria using processes designed to ensure compliance with technical standards currently exists.

Additionally, such audits may expose sensitive operational details and user data, raising privacy and security risks. For instance, the report requires that “All personal data contained in the report... shall be deidentified and aggregated,” and requires the disclosure of “how the covered online service provider utilized algorithms.” Such mandatory disclosures jeopardize both user privacy and covered services’ proprietary information without a framework in place to safeguard these potentially sensitive disclosures.

* * * * *

We appreciate your consideration of CCIA’s comments and stand ready to provide additional information as you consider proposals related to technology policy.

Sincerely,

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

⁹ See, e.g., *FASAB Handbook of Federal Accounting Standards and Other Pronouncements, as Amended*, Fed. Acct. Stds. Advisory Bd. (June 30, 2025), available at <https://fasab.gov/accounting-standards/> (specifying processes for demonstrating compliance with the Generally Accepted Accounting Principles (GAAP)).