July 1, 2026

The Honorable Mikie Sherrill
Governor of New Jersey
125 West State Street
Trenton, NJ 08625

Re: A 4015 - "New Jersey Kids Code Act" (Veto Request)

Dear Governor Sherrill,

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto of 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 Amendment.

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 Inst., *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).

Other aspects of the bill restrict free speech as well. An Arkansas federal court recently enjoined time-based notification restrictions on online services, holding that they "[burden online services'] speech by silencing them for a third of the day without any indication that the burden will reduce nighttime social media use or otherwise serve the State's asserted interest at all".[5] Notably, such restrictions prevent family messages, emergency alerts, and school closure notifications. The same decision enjoined mandatory default settings that bar adults from communicating with minors, holding that they "suppress lawful speech as the means to suppress unlawful speech."[6] However, A 4015 prohibits covered operators from sending notifications to minors at specific times of day, and from "displaying media created or posted by the covered minor to another user the covered online service provider knows to be an adult" as a default setting. These restrictions suppress lawful speech as well as unlawful speech and are therefore unconstitutional.

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.[7] 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.[8]

The bill's requirements are not well-defined.

A 4015 is not specific regarding online services' obligations. The bill defines "covered design feature" in highly subjective terms. It is difficult to objectively determine when a design feature "motivates or causes more frequent or more extensive use of an online service through incentives or frequency of use," "emulates gameplay," "facilitates a false perception of an image," or "increase[s] usage through the illusion of talking with a human being that seeks to elicit feelings of intimacy from the user." Such definitions require making imprecise and subjective assessments regarding a given feature's impact on a user's emotional state. They also require regulators and courts to decide which features are responsible for a user's increased time spent using a service, which is virtually impossible to objectively measure. Moreover, "covered design feature[s]" are explicitly "not limited to" the listed criteria, making the term even less definite. Defining covered services' compliance obligations using such vague terms risks arbitrary and inconsistent application of the law.

---

[5] *NetChoice v. Griffin*, No. 5:25-CV-5140, 2026 WL 1068565 at *17 (W.D. Ark. Apr. 20, 2026).
[6] *Id.* at *19 (quoting *Packingham v. North Carolina*, 582 U.S. 98, 106 (2017)).
[7] 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/.
[8] 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/.

It is also unclear how conflicts between A 4015 and existing laws are to be resolved. Section 18.b provides that when the bill conflicts with another state law, "the law that affords the greatest protection from harm to minors controls." Often it will be unclear which law "affords the greatest protection," leaving covered services to guess which law they must follow.

Furthermore, most privacy laws that prohibit the use of "dark patterns" do so only in specific contexts, such as to obtain consent.[9] 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.

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 the time 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.

[9] *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 discourages investments in online safety.

The bill's duties apply whenever a covered provider knows a user's age, determined in part based on "any age the covered online service provider has attributed or associated with the individual for any purpose, including... product development." This provision creates legal risk specifically for companies who develop online safety features for minors. To develop such features, covered businesses will likely have to gather data about users' ages, and thus subject themselves to the requirements in this bill. By contrast, those who avoid such investments can escape these obligations. Legislation should reward investments in online safety rather than deterring it by tying such investments to additional legal and compliance burdens.

The bill requires audits without an appropriate framework in place.

Section 13 provides that a 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 specifications[10] 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.

Furthermore, the auditing process requires an extensive, technically sophisticated compliance regime that will disproportionately burden smaller businesses. The bill requires sorting online services' user base with unprecedented levels of granularity. Many covered services do not possess the technical capabilities to compile the required data. The requested level of detail thus undermines competition without tangibly benefitting consumers.

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.

If enacted, A 4015 may result in denying services to all users under 18, limiting their access to needed supportive communities.

The bill's lack of narrowly tailored definitions 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

[10] *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)).

like-minded individuals and communities. For minors in unsafe households or from minority groups who may not have local peers with shared experiences, digital services can provide vital communities for support and resources.[11]

* * * * *

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

[11] *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/.