January 22, 2026

The Honorable Henry McMaster
Governor South Carolina
1100 Gervais Street
Columbia, SC 292010

Re: [HB 3431] - "Age Appropriate Design Code" (Oppose)

Dear Gov. McMaster:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully urge you to veto HB 3431 as enrolled on January 21, 2026. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. 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.[1] However, while CCIA shares the goal of increasing online safety for minors, the updated language of HB 3431 introduces significant constitutional, operational, and privacy concerns that would negatively impact South Carolina residents and businesses.

HB 3431'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."[2] However, HB 3431 mandates specific design requirements and prohibits certain commonly used features such as notifications and engagement mechanisms. By broadly controlling how services organize, present, and prioritize information to users, the bill creates content-based restrictions on speech that raise serious First Amendment concerns.

Moreover, HB 3431 regulates online services based on whether they are "reasonably likely to be accessed by minors." Multiple federal courts have found regulating online services on this basis to be unconstitutional. Last year a federal court found that a California law regulating providers on this basis was "content-based on its face"[3] and "likely to fail strict scrutiny."[4] Months later, an Ohio court found such language to be unconstitutionally vague in violation of

[1] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated June 10, 2025).
[2] *Moody v. NetChoice*, 144 S. Ct. 2383, 2408 (2024).
[3] *NetChoice v. Bonta*, 770 F. Supp. 3d 1164, 1186 (N.D. Cal. 2025).
[4] *Id.* at 1195.

the Fourteenth Amendment, noting that "this expansive language would leave many operators unsure as to whether it applies to their website."[5]

The bill's requirements are not well-defined.

Not only is it difficult for online services to determine whether HB 3431 would apply to them, it is also difficult to ascertain their specific responsibilities if it does. The bill requires covered services to "exercise reasonable care" in mitigating a broad list of defined harms in the creation and implementation of design features. However, it is unclear what obligations this provision confers in practice, leaving covered services unable to know whether they are violating the law.

The same is true of the term "compulsive usage," defined as "the persistent and repetitive use of a covered online service that substantially limits one or more of a user's major life activities including, but not limited to, sleeping[,] eating, learning, reading, concentrating, communicating, or working." The bill does not specify what constitutes persistent and repetitive use, substantial limitation of the above activities, or a link between the two. Consequently, covered entities will have no way of knowing what measures they need to institute, or how they are to know whether they are succeeding. Defining covered services' obligations using such vague and subjective terms risks arbitrary and inconsistent application of the law.

The bill's scope is overly broad.

HB 3431 covers any business who "annually buys, receives, sells, or shares the personal data of fifty thousand or more consumers, households, or devices…." 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.

Furthermore, many of the terms used to describe these compliance obligations are defined far more broadly than their generally accepted meanings. "Personalized recommendation system" is defined such that virtually any method of ordering content would qualify. Moreover, the term is used in regulations that apply to all users, not just minors. The term "notifications and push alerts" is not defined at all, and could apply to emails or security alerts. Implementing these complex requirements is a costly endeavor which would deter small businesses from scaling up their operations and do little to protect users online.

[5] *NetChoice v. Yost*, 778 F. Supp. 3d 923, 957 (S.D. Ohio 2025).

The bills require audits without an appropriate framework in place.

Section 2(b) 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 covered online service as it pertains to minors, including its covered design features, its use of personal data, and its business practices as they pertain to minors." Formal audits, however, are intended to demonstrate compliance with detailed sets of specifications[6] rather than general principals. Audits are not designed to evaluate subjective criteria such as whether a provider is "likely to be accessed by minors" or "will encourage or increase a minor's frequency, time spent, or activity on a covered 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.

* * * * *

CCIA recommends that you veto legislation that risks being invalidated in court, thereby avoiding burdening businesses and passing on expensive litigation costs to taxpayers. We encourage you to urge the Legislature to consider alternative approaches, such as digital citizenship curricula, that empower parents and children without compromising constitutional rights or online privacy.

Sincerely,

Tom Mann
West State Policy Director
Computer & Communications Industry Association

[6] *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)).