March 11, 2026

Senate Committee on Finance, Insurance, and Consumer Protection
Attn: Michael Sitkauskas
Binsfeld Office Building
201 Townsend St
Lansing, MI 48933

Re: SB 758 - "Kids Code Act" (Oppose)

Dear Chair Cavanagh and Members of the Senate Finance, Insurance, and Consumer Protection Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 758. 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, SB 758 introduces significant constitutional, operational, and privacy concerns that would negatively impact Michigan residents and businesses.

SB 758'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, SB 758 requires the Michigan Attorney General to institute "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

[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).

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.

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.[5] SB 758, however, does not contextualize the prohibition on "dark patterns." Without such contextual information, prohibiting interface designs "with the effect of substantially impairing a covered minor's autonomy, decision making, 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 incentivizes overcollection of minors' data.

SB 758 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 during the school year, 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's scope is overly broad.

SB 758 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 and engage in location-based tracking of their users if they use any notifications. To achieve compliance, this vast array of businesses will require significant technical capabilities that many businesses may not possess. A coffee shop, for instance, might be subjected to the audit requirements and design feature restrictions in the bill.

The bill requires audits without an appropriate framework in place.

Section 17 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 covered online

[4] *See, e.g.*, *NetChoice v. Bonta*, 152 F.4th 1002, 1016-17 (9th Cir. 2025).
[5] *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.

service provider as pertaining to minors, including the online service's covered design features, the use of personal data, and business practices." Formal audits, however, are intended to demonstrate compliance with detailed sets of specifications[6] 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… must 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.

* * * * *

CCIA remains committed to working with the Michigan Legislature on constructive, evidence-based approaches to online safety. We appreciate your consideration of these comments and stand ready to provide additional information as you consider proposals related to technology policy.

We thank you for your consideration of these comments.

Sincerely,

Megan Stokes
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)).