February 6, 2026

Banking, Commerce and Insurance Committee
1445 K St
Lincoln, NE 68508

Re: LB 1119 - "Age-Appropriate Online Design Code Act" (Oppose)

Dear Chair Jacobson and Members of the Banking, Commerce and Insurance Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose LB 1119. 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, while CCIA shares the goal of increasing online safety for minors, LB 1119 (which would amend last Session's LB 504, also named the Age-Appropriate Online Design Code Act, which CCIA opposed)[3] introduces significant constitutional, operational, and privacy concerns that would negatively impact Nebraska residents and businesses.

LB 1119's method of designating covered services violates the First Amendment.

In 2024, the Supreme Court ruled that "regulating the content-moderation policies" of websites "to change the speech that will be displayed there… is a preference" that states "may not impose."[4] However, LB 1119 requires numerous design requirements that restrict what content covered services can display, including "providing a visible count of how many likes, comments, clicks, views, or reactions a user-generated item has received," a mandate that federal courts have found to violate the First Amendment.[5] 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] Megan Stokes, *CCIA Comments Opposing NE LB 504* (Feb. 3, 2025), https://ccianet.org/library/ccia-comments-on-ne-lb-504/.
[4] *Moody v. NetChoice*, 144 S. Ct. 2383, 2408 (2024).
[5] *See, e.g.*, *NetChoice v. Bonta*, 152 F.4th 1002, 1016-17 (9th Cir. 2025).

The bill's requirements are not clear or well-defined.

It is difficult for covered services to ascertain their responsibilities under LB 1119. The term "covered design feature," which was part of LB 504, continues to be defined as "any feature or component of a covered online service that will encourage or increase the frequency, time spent, or activity of a user", a provision that could in theory apply to *any* of a service's design features, since any new capabilities a feature provide will likely create additional reasons for users to use the covered service. However, although LB 1119 still defines this term, any provisions from LB 504 regarding it have been removed, and no remaining regulatory provision appears to use it. Accordingly, it is unclear what obligations covered services have regarding such features, leaving covered services unable to know whether they are violating the law.

Besides failing to clarify which regulations apply to "covered design feature[s]," the bill defines many of these features using vague 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 "increases 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. Moreover, they 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. Defining covered services' compliance obligations using such vague terms risks arbitrary and inconsistent application of the law.

Furthermore, most privacy laws that prohibit the use of "dark patterns" do so only in specific contexts, such as to obtain consent.[6] LB 1119, 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.

LB 1119 greatly expands the scope of covered entities from LB 504 and now regulates any covered online service who "annually processes the personal data of fifty thousand or more consumers, households, or devices, alone or in combination with its affiliates, subsidiaries, or parent companies." 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 the many restrictive design features required by this bill, requiring significant technical capabilities that many smaller businesses may not possess.

[6] *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.

* * * * *

While we share the concerns of the sponsor and the Banking, Commerce and Insurance Committee regarding the safety of young people online, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. We appreciate the Committee's consideration of these comments and stand ready to provide additional information as Nebraska considers proposals related to technology policy.

Sincerely,

Megan Stokes
Director of State Policy
Computer & Communications Industry Association