



April 14, 2026

Nebraska Legislature  
1445 K St  
Lincoln, NE 68508

**Re: LB 838 - "Change provisions relating to the financial exploitation of vulnerable or senior adults, rules and codes of procedure, decedents' estates, inheritance taxes, deceptive trade practices, the Age-Appropriate Online Design Code Act, the Equipment Business Regulation Act, the Nebraska Money Transmitters Act, and the Nebraska Uniform Trust Code and provide for rounding of certain cash transaction amounts" (Oppose)**

Dear Governor Pillen:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto of LB 838. Our opposition is specifically to the language that was originally in LB 1118 and LB 1119, which we also opposed.<sup>1</sup> CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.<sup>2</sup> 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.<sup>3</sup> However, while CCIA shares the goal of increasing online safety for minors, LB 838 (which, among other things, would amend last Session's LB 504, also named the Age-Appropriate Online Design Code Act, which CCIA opposed)<sup>4</sup> introduces significant constitutional, operational, and privacy concerns that would negatively impact Nebraska residents and businesses.

---

<sup>1</sup> CCIA Opposes Nebraska Bill That Would Expand Deceptive Trade Practices Law and Harm Small Businesses (Feb. 10, 2026),

<https://ccianet.org/news/2026/02/ccia-opposes-nebraska-bill-that-would-expand-deceptive-trade-practices-law-and-harm-small-businesses/>; CCIA Warns Nebraska Legislature that LB 1119 Raises Constitutional and Privacy Concerns (Feb. 9, 2026),

<https://ccianet.org/news/2026/02/ccia-warns-nebraska-legislature-that-lb-1119-raises-constitutional-and-privacy-concerns/>.

<sup>2</sup> 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>.

<sup>3</sup> Competitive Enterprise Institute, *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/> (last updated June 10, 2025).

<sup>4</sup> Megan Stokes, *CCIA Comments Opposing NE LB 504* (Feb. 3, 2025), <https://ccianet.org/library/ccia-comments-on-ne-lb-504/>.



LB 838 would also undermine existing work to combat fraudulent advertising. Responsible digital services partner with a wide range of stakeholders to protect consumers from illegal and dangerous content and conduct online, including fraudulent advertisements. They participate in voluntary information sharing programs and educational campaigns to assist in detecting, reporting, identifying, and removing fraud and other illegal or dangerous content. There is close coordination with federal, state, and local law enforcement to better identify bad actors, hold them accountable, and prevent misconduct. Companies will reject ads that violate their policies (e.g., spam, phishing scams, manipulated media, and other deceptive practices), as well as review and take action on existing accounts and posts in response to user reports. For companies operating at scale, that may be tens of millions of pieces of content. While addressing fraud is a priority for CCIA members, LB 838 would undermine these existing industry efforts by imposing infeasible prescriptive mandates that will ultimately harm Nebraska consumers and businesses.

## **LB 838’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.”<sup>5</sup> However, LB 838 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.<sup>6</sup> 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 undermine competition.**

Requiring covered entities to investigate and determine the status of allegedly fraudulent advertisements within seven days, regardless of complexity, and to take them down “immediately” could incentivize over-removal of lawful content to avoid liability. This approach would harm legitimate advertisers, including small businesses, and reduce consumer access to lawful products and services in Nebraska.

These extensive compliance obligations would require significant technical, legal, and staffing resources, creating barriers to entry and reducing competition in the digital advertising marketplace. These actions are contrary to Nebraska’s pro-innovation and pro-business values. By prioritizing formal compliance checklists over flexible, risk-based approaches, LB 838 may divert resources away from the most effective fraud prevention tools and partnerships currently in use.

## **The bill’s requirements are not clear or well-defined.**

It is difficult for covered services to ascertain their responsibilities under LB 838. The term “covered design feature,” which was part of LB 504, continues to be defined as “any feature or

<sup>5</sup> *Moody v. NetChoice*, 144 S. Ct. 2383, 2408 (2024).

<sup>6</sup> *See, e.g., NetChoice v. Bonta*, 152 F.4th 1002, 1016-17 (9th Cir. 2025).

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 838 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.<sup>7</sup> LB 838, 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 would make it a “deceptive trade practice” for a covered “social media platform” to fail to establish and implement a long list of burdensome programs and processes, many of which are undefined or subjective. Terms such as “unlawful impersonation detection and mitigation,” “automated and manual fraud detection systems,” “measures to prevent repeated offenses,” and “ignores credible reports” lack clear statutory benchmarks, exposing covered entities to liability based on hindsight rather than reasonable, good-faith efforts.

### **The bill’s scope is overly broad.**

LB 838 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

<sup>7</sup> 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](https://www.cga.ct.gov/2024/sup/chap_743jj.htm).



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.

**The bill raises conflicts with federal law and will not stop fraud.**

This proposal would regulate services that are inherently interstate, and can only effectively be addressed at the federal level. Moreover, targeting one specific subset of online ads for regulation will inevitably raise costs in order to ensure compliance, likely resulting in bad actors going elsewhere (e.g., ad-supported games, which are carved out), or offline, where these onerous know-your-customer rules don't apply.

\* \* \* \* \*

While we share the concerns of the Nebraska Legislature regarding the safety of individuals online, we encourage lawmakers to resist advancing legislation that is not adequately tailored to this objective. We 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