March 18, 2026

Nebraska Legislature
1445 K St
Lincoln, NE 68508

Re: LB 1083 - "Adopt the Transparency in Artificial Intelligence Risk Management Act, create a fund, and change provisions relating to records which may be withheld from the public" (Oppose)

Dear Senator Storer:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose LB 1083. 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.

While CCIA shares the Legislature's commitment to protecting consumers, minors, and prioritizing personal privacy and youth safety, LB 1083 would impose an expansive and fragmented regulatory regime that risks chilling innovation, undermining free expression, and placing Nebraska significantly out of step with recommended federal and international approaches to artificial intelligence governance.[2] By comparison, LB 1185 requires clear disclosures and implements a framework that gives innovative businesses what they need to ramp up operations within the state. A light-touch, practical framework gives tech companies a way to understand the rules and invest capital, boosting Nebraska's economy.[3]

LB 1083 contains an overly broad and vague regulatory scope and definitions.

LB 1083 incorrectly combines frontier-model safety requirements with child-safety obligations into a single "public safety and child protection plan." Both of these efforts require fundamentally different regulatory approaches. There are multiple entities involved in an AI system, including developers, deployers, users, hardware, and software. It is crucial to correctly assign liability among them. Legislation should ensure that developers and deployers are not held liable for the harmful actions of users. Similarly, end-users should not be responsible for intentionally created flaws in an AI model, such as one that consistently produces biased outcomes. Correctly assigning responsibility ensures that liability falls on the party best positioned to prevent harm and be held accountable for any damages.

---

[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] CCIA, *Understanding AI: A Guide To Sensible Governance* (June 2023), https://ccianet.org/library/understanding-ai-guide-to-sensible-governance/.

[3] Heath Mello, *Guest Editorial: Support Nebraska Business with LB 1185*, Silicon Prairie News (Feb. 21, 2026), https://siliconprairienews.com/2026/02/guest-editorial-support-nebraska-business-with-lb-1185/.

The bill relies on broad and imprecise definitions of "artificial intelligence," "frontier model," "large chatbot provider," and "artificial intelligence model" that would encompass a vast range of common digital tools, including customer service chat functions, workplace productivity software, educational platforms, accessibility technologies, and automated moderation or safety tools. These technologies differ significantly in function, risk profile, and user interaction, yet the bill treats them as functionally equivalent.

Key definitions like "severe emotional distress" remain undefined as well, which would result in applying highly subjective standards to AI systems. These kinds of standards create compliance uncertainty and make it impossible for covered services to know if they are meeting requirements.

The absence of clear, administrable boundaries makes it difficult for companies to determine whether their products fall within the scope of the bill or which obligations apply. Faced with ambiguous standards and significant penalties, providers are likely to respond by limiting features, restricting access, or withdrawing services entirely rather than attempting to interpret and comply with unclear requirements. This approach ultimately reduces consumer choice and limits access to beneficial technologies without meaningfully advancing safety or privacy objectives.

LB 1083 contemplates "industry-consensus best practices" as part of covered entities' "public safety and child protection plan." This is important as "best practices" in AI governance and technology policy more broadly are not solely a matter of government preference, and should not be dictated by prescriptive regulations. Meaningful best practices require consultation with industry stakeholders who design, deploy, and operationalize these systems, along with the relevant stakeholders who understand how AI functions in real-world settings.[4] The safeguards, tools, and governance approaches that best mitigate risk are those that are principle-based and readily adaptable to the constantly-evolving nature of AI and like technologies.

Consumer-facing digital services have already built considerable consensus around mitigating risk to users and other parties. A recently published international standard, ISO/IEC 25389, reflects the evolving industry consensus on mitigating online risk.[5] This reflects the first horizontal standard for safety on online consumer services. Insofar as there is work occurring in this space, it should incorporate the existing consensus around best practice: safety by design, appropriate governance, application, iteration, and improvement, and transparency.

LB 1083's requirements misunderstand the AI ecosystem and risk creating a patchwork regulatory environment.

The January 1, 2027, effective date gives companies less than 11 months to develop the comprehensive compliance programs required by the bill. Asking covered services to build

[4] *See, e.g.*, Digital Trust & Safety Partnership, *Best Practices for AI and Automation in Trust and Safety* (Sept. 2024), https://dtspartnership.org/best-practices-for-ai-and-automation-in-trust-and-safety/.
[5] ISO/IEC 25389:2025, Information technology — The safe framework (Edition 1, June 2025), https://www.iso.org/standard/90106.html.

compliance programs while the regulatory framework itself is still evolving due to the Attorney General assessing and updating definitions with the same deadline, is impossible.

The "large frontier developer" definition links model risk to company size, relying on annual revenue benchmarks. Models created by small and large developers alike run the same risks regardless of who develops them. Such penalties and obligations should be tied to the frontier model itself rather than corporate revenues.

The bill would also contribute to a growing patchwork of state artificial intelligence laws that impose inconsistent and potentially conflicting obligations on interstate digital services. Artificial intelligence systems are developed, trained, and deployed on a national and global scale. Prescriptive state-level mandates risk becoming outdated quickly, complicating compliance, and discouraging investment in jurisdictions that adopt rigid or punitive frameworks. A fragmented regulatory approach threatens that position by making it more difficult for companies to deploy new services and features in the state.

The bill's private right of action and harsh penalties would result in the proliferation of frivolous lawsuits, questionable claims, and exorbitant statutory damages.

LB 1083 permits "an aggrieved employee or applicant" to "institute a civil action" against a wide range of "large frontier developers." The bill would enable "appropriate relief, including temporary or permanent injunctive relief, general and special damages, and reasonable attorney's fees and court costs per violation."

The bill also establishes penalties up to $1 million per violation for large frontier developers with no cure provision. This, combined with subjective standards throughout the bill, means companies acting in good faith could face massive financial penalties for conduct they reasonably believed was compliant. While AI may introduce new considerations that warrant careful attention, these risks are best addressed through flexible frameworks that evolve alongside technology.

By creating a new private right of action, the measure would open the doors of state courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. As lawsuits prove extremely costly and time-intensive, it is foreseeable that these costs would be passed on to individuals in Nebraska, disproportionately impacting smaller businesses and startups across the state.[6]

* * * * *

While we share your concerns regarding the safety of individuals online, we encourage you to resist advancing legislation that is not adequately tailored to this objective. We stand ready to provide additional information as you consider proposals related to technology policy.

[6] Trevor Wagener, *State Regulation of Content Moderation Would Create Enormous Legal Costs for Platforms*, Broadband Breakfast (Mar. 23, 2021), https://broadbandbreakfast.com/trevor-wagener-state-regulation-of-content-moderation-would-create-enormous-legal-costs-for-platforms/.

Sincerely,

Megan Stokes
Director of State Policy
Computer & Communications Industry Association