

LB 383, the Parental Rights in Social Media Act

LETTER OF OPPOSITION

April 10, 2025

Dear Senators,

On behalf of NetChoice, a national trade association working to make the internet safe for free enterprise and free expression, we write to express our opposition to LB 383, which would ban social media for those under 18 without parental consent, and require all users of social media to verify their ages, among other provisions.

We share the sponsor's goal to better protect minors from harmful content online. NetChoice members have taken issues of teen safety seriously and in recent years have rolled out numerous new features, settings, parental tools, and protections to better empower parents and assist in monitoring their children's use of social media. We ask that you oppose LB 383 and instead use this bill as a way to jumpstart a larger conversation about how best to protect minors online and consider alternatives that do not raise constitutional issues.

Key Concerns:

1. LB 383 imposes unconstitutional age-verification and parental consent requirements;
2. Age-verification and parental consent presents heightened threats to privacy and undermines the state's interest in protecting the privacy of minors.
3. LB 383 includes a troubling private right of action that invites abusive litigation.

LB 383's core provisions are unconstitutional and are already being actively litigated in other states:

The bill's restrictions on minors' access to social media platforms raise First Amendment concerns by limiting their ability to access information and engage in protected speech. Courts have consistently recognized that minors have constitutional rights to receive information and ideas through various media. The bill's requirements would effectively create a barrier to constitutionally protected speech, as platforms would be required to verify age before allowing access to any content. This constitutes a prior restraint on speech, which courts have traditionally viewed with particular skepticism. Similar provisions

have been challenged in federal court and laws in Utah, Mississippi, Arkansas, and Ohio are currently enjoined.

Additionally, the Supreme Court has invalidated parental consent requirements when they impermissibly chill access to lawful speech.¹ In *Brown v. Entertainment Merchants Association*, the Court struck down a California law restricting minors' access to violent video games without parental consent. The Court rejected the notion that a new category of unprotected speech could be created for speech directed at children, emphasizing that minors are entitled to significant First Amendment protection. Justice Scalia's majority opinion noted that the government cannot "restrict the ideas to which children may be exposed" simply because it disagrees with them.

When other courts have examined age-verification and parental consent laws, *Brown* governs. For example, when the District Court for the Southern District of Ohio reiterated that parental consent laws do not enforce parental authority but enforces *governmental* authority subject to a parental veto. "[Ohio's parental consent law] appears to be exactly that sort of law. And like content-based regulations, laws that require parental consent for children to access constitutionally protected, non-obscene content, are subject to strict scrutiny."²

Age-Verification and parental consent requirements undermine privacy:

We share the legislature's goal of protecting young people online, however LB 383's approach would create significant privacy and security concerns while potentially limiting beneficial online interactions for Nebraska's youth.

While Section 3(1)(b) prohibits companies from retaining identifying information "after verification is complete," this provision is both vague and impractical. The bill fails to define when verification is "complete," especially for ongoing accounts that may require reverification.

The bill effectively requires every internet user—regardless of age—to submit personal documentation, such as a government-issued ID, to access social media. This means websites would need to collect and store sensitive information, creating massive databases that will inevitably become targets for hackers. This runs counter to best practices of data minimization and could make Nebraska residents more susceptible to identity theft and fraud.

As we have seen, no number of safeguards can ensure against data breaches. According to Child Identity Fraud Reports from Javelin Strategy and Research, nearly 2 million children were victims of identity theft in 2022³. Meanwhile, the 2019 hack of Pearson (a school technology provider) exposed information of

¹ *Brown v. Entertainment Merchants Ass'n*, 564 U.S. 786 (2011).

² *NetChoice v. Yost*, 716 F. Supp. 3d 539, 558 (S.D. Ohio 2024).

³ Javelin, *1.7 Million U.S. Children Fell Victim to Data Breaches According to Javelin's 2022 Child Identity Fraud Study*, (Oct. 26, 2022) (last visited Mar. 22, 2024),

thousands of children, including their names, birthdates, and email addresses.⁴ Even government agencies responsible for storing personal information have been subject to massive data leaks.⁵ Mandating that websites or services collect sensitive personal data on minors as a precondition for accessing vast swaths of online speech substantially increases these risks. They also make websites juicier targets for hackers.

Accordingly, state legislatures should evaluate whether their proposed policies would advance privacy protections or simply subject minors and adults to greater vulnerability in their online lives.

Finally, Section 4 of LB 383 creates a troubling private right of action that invites abusive litigation. By allowing any "person aggrieved" to bring civil action with potential recovery of attorney's fees, the bill establishes financial incentives for opportunistic lawsuits. This provision would overwhelm Nebraska's court system while forcing online services to implement overly restrictive measures to avoid costly litigation. The vague standard of "actual damages" for non-data-retention violations leaves businesses with uncertain liability exposure, discouraging innovation and service provision in Nebraska.

An Approach that Actually Works

Rather than enact clearly unconditional laws banning the free speech of Nebraska residents, the state would be better served enacting laws that help the citizens and are legal. NetChoice is working with lawmakers from across the country to achieve such ends.

Requiring Digital Education in Schools

We strongly support the bill's education provisions. Empowering students with digital literacy skills and knowledge about online safety through curriculum developed by education experts represents a constitutional and effective approach. The curriculum requirements effectively address crucial issues facing young people online, including mental health impacts, content manipulation, digital permanence, and identifying dangerous behaviors like cyberbullying, predatory conduct, and human trafficking. The reporting mechanisms ensure students know how to get help when needed. This approach will not only reach children where they are, but will help arm them to become better digital citizens.

Many online platforms have implemented robust parental control features. For example, some online platforms have led the way with impressive suites of tools for parents and teens to better protect themselves. Additional parental controls are available at the device level. For example, iPhones and iPads empower parents to limit the amount of time their children can spend on the device, choose which applications (e.g., YouTube, Facebook, Snapchat, or Instagram) their children can use, set age-related content restrictions for those applications, filter online content, and control privacy settings. This

⁴ Lindsay McKenzie, *Pearson Hack Exposes Thousands of Students' Data*, INSIDE HIGHER ED (Aug. 4, 2019), <https://www.insidehighered.com/quicktakes/2019/08/05/pearson-hack-exposes-thousands-students%E2%80%99-data>.

⁵ Sean Lyngaas, *Millions of Americans' personal data exposed in global hack*, CNN POLITICS, June 16, 2023, <https://www.cnn.com/2023/06/16/politics/cyberattack-us-government/index.html>.

market-driven approach encourages innovation and allows for diverse solutions that can cater to different needs and preferences.

Updating Child Abuse Laws for AI

Today, child abusers are able to use artificial intelligence to create images and escape justice under existing Child Sexual Abuse Material (CSAM) laws. This is because existing CSAM laws require real images of the abuse, rather than AI generated ones. NetChoice is working with lawmakers to create laws that fill the gaps in existing CSAM laws to protect children from such abuses.

Empowering law enforcement to arrest child abusers

Today less than 1% of all reports of child abuse are even investigated. That means that 99% of reports of child abuse go unheard. This is because law enforcement doesn't have the resources it needs to investigate and prosecute child abusers. NetChoice supports giving law enforcement the resources it needs to put child abusers behind bars.

Given the constitutional problems presented by age-verification and parental consent, NetChoice urges you to **oppose LB 383** to avoid identical constitutional pitfalls. Instead, we respectfully ask you to work with industry stakeholders to develop more effective approaches to protecting young people online while preserving their privacy and access to beneficial digital services. As always, we offer ourselves as a resource to discuss any of these issues with you in more detail.

Sincerely,

Amy Bos

Director of Federal and State Affairs

NetChoice is a trade association that works to protect free expression and promote free enterprise online.