



April 16, 2024

Office of the Honorable Governor Bill Lee
State Capitol, First Floor
600 Charlotte Avenue
Nashville, TN 37243

RE: HB 1891 – “AN ACT to amend Tennessee Code Annotated, Title 47, Chapter 18, relative to protecting minors from social media.” (Veto Request)

Dear Governor Lee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto on HB 1891.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.¹ CCIA holds a firm conviction that children are entitled to a higher level of security and privacy in their online experiences. Presently, our members are actively engaged in various initiatives to integrate robust protective design features into their websites and platforms.² CCIA’s members have been leading the effort to implement settings and parental tools to individually tailor younger users’ online use to the content and services that are suited to their unique lived experience and 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 to allow parents to block specific sites entirely.³

This is also why CCIA supports the implementation of digital citizenship curriculum in schools, to not only educate children on proper social media use but also help educate parents on what mechanisms presently exist that they can use now to protect their children the way they see fit and based on their family’s lived experiences.⁴

It should also be recognized that protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Speech that is neither obscene to young people nor subject to other legitimate laws cannot be suppressed solely to protect young online users from ideas or images that a legislative body disfavors. Proposals to keep children safe online should be established through a risk-based approach to developing protections for different ages of users and by focusing on tangible harm. While CCIA shares the goal of increasing online safety, HB 1891 presents the following concerns.

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 Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children’s Safety Online*, Disruptive Competition Project (Feb. 7, 2023), <https://www.project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/>.

³ Competitive Enterprise Institute, *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/>.

⁴ See supra note 2.



HB 1891's provisions regarding liability for data collection and age verification will not achieve the bill's stated objectives.

HB 1891 would hold covered social media companies liable for failing to perform age verification but also prohibits a social media company from retaining any personal identifying information about the user after verifying their age. However, by requiring covered businesses to delete relevant information, the law would leave businesses without a means to document their compliance. This becomes especially problematic in instances where a user decides to use deceptive verification information such as using an identification card that is not their own. Additionally, it is also unclear what impact users' employment of virtual private networks (VPNs)⁵ and other mechanisms to avoid location-specification age verification requirements could have on organizations' liability under this bill. It does not advance the bill's goal to place covered companies in a Catch-22 where they cannot be fully compliant without incurring new liability.

More broadly, the bill's obligation to collect additional information associated with age verification is itself likely to conflict with data minimization principles inherent in typical federal and international privacy and data protection compliance practices. If the state were to force companies to collect a higher volume of data on users even as others are requiring the collection of less data, it may place businesses in an untenable position of picking which state's law to comply with, and which to unintentionally violate.⁶ A recent study from the Pew Research Center found that many Americans worry about children's online privacy but when asked about who is responsible for protecting children's online privacy, most (85%) say parents hold a great deal of responsibility for protecting kids' online privacy. 59% also say that tech companies bear the responsibility while 46% believe the government does. The study also highlights why it is important to consider the tradeoffs associated with age verification and consent proposals that would require additional collection data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.

Further, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification solutions but found that none of these options could satisfactorily meet three key standards: 1) providing sufficiently reliable verification; 2) allowing for complete coverage of the population, and; 3) respecting the protection of individuals' data, privacy, and security.⁷ Though the intention to keep kids safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people.

⁵ Cristiano Lima, *Utah's porn crackdown has a VPN problem*, The Washington Post (May 5, 2023), <https://www.washingtonpost.com/politics/2023/05/05/utahs-porn-crackdown-has-vpn-problem/>.

⁶ Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard>.

⁷ *Online age verification: balancing privacy and the protection of minors*, CNIL, (Sept. 22, 2022), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors>.

Restricting access to the internet for younger users curtails their First Amendment right to information, denying them entry to supportive online communities that might be unavailable in their local physical location.

The Children’s Online Privacy Protection Act (COPPA) and associated rules at the federal level currently regulate how to address users under 13, a bright line that was a result of a lengthy negotiation process that accounted for the rights of all users, including children, while also considering the compliance burden on businesses. To avoid collecting data from users under 13, some businesses chose to shut down various services when COPPA went into effect due to regulatory complexity — it became easier to simply not serve this population. Users under 18 could face a similar fate as HB 1891 would implement more complex vetting requirements tied to parental consent and age verification.

When businesses are required to deny access to social networking sites or other online resources, this may also unintentionally restrict children’s ability to access and connect with like-minded individuals and communities. For example, in instances where children may be in unsafe households, this could create an impediment for children seeking communities of support or resources to get help.

Serious concerns also arise when verifying whether a “parent, guardian, or person who has custody of, or person who has caregiving authority over” is, in fact, a minor’s legal parent or guardian. Many parents and legal guardians do not share the same last name as their children due to remarriage, adoption, or other cultural or family-oriented decisions. If there is no authentication to confirm whether an individual is actually a minor’s legal parent or guardian, this may incentivize minors to ask other adults who are not their legal parent or guardian to verify their age on behalf of the minor to register for an account with a social media company. It is also unclear who would be able to give consent to a minor in foster care or other nuanced familial situations, creating significant equity concerns. Further, scenarios where a legal parent or guardian is not located in Tennessee or is not a resident of the state creates significant confusion for consumers and businesses.

Age verification and parental consent requirements for online businesses are currently being litigated in several jurisdictions.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.⁸ After 25 years, age authentication still remains a vexing technical and social challenge.⁹ California, Arkansas, and Ohio recently enacted legislation that would implement age verification and estimation requirements — each law is currently facing a legal challenge due to constitutional concerns, and judges recently put both laws on hold until these challenges can be fully reviewed.¹⁰ The fate of a similar law in Utah is also in jeopardy as it is also facing legal

⁸ *Reno v. ACLU*, 521 U.S. 844 (1997).

⁹ Jackie Snow, *Why age verification is so difficult for websites*, The Wall Street Journal (Feb. 27, 2022), <https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728>.

¹⁰ *NetChoice, LLC v. Bonta* (N.D. Cal. 5:22-cv-08861); *NetChoice, LLC v. Griffin* (W.D. Ark. 5:23-cv-05105); *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047)).



challenges.¹¹ **CCIA believes that the existing age verification and parental consent requirements under HB 1891 are likely to raise similar constitutional concerns and significantly fail to meet constitutional standards.** CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated and passing on *expensive litigation costs to taxpayers*.

* * * * *

While we share your concerns regarding the safety of young people online, we encourage you to resist signing legislation that is not adequately tailored to this objective, and we respectfully request a veto of HB 1891.

We appreciate your consideration of these comments and stand ready to provide additional information related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

¹¹ *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).