March 19, 2024

Senate Labor, Commerce and Industry Committee
Attn: Julie DesChamps, Administrative Assistant
Room 203, Gressette Building
1101 Pendleton Street
Columbia, SC 29201

RE: HB 4700 - "South Carolina Social Media Regulation" (Oppose)

Dear Chair Davis and Members of the Senate Committee on Labor, Commerce and Industry:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 4700 in advance of the Senate Committee on Labor, Commerce and Industry hearing on March 20, 2024.

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. In recent sessions, there has been a notable surge in state legislation concerning children's online safety. Acknowledging policymakers' valid concerns about the online privacy of young individuals, it is imperative to prioritize the establishment of a comprehensive data privacy law applicable to all consumers. This law should incorporate safeguards for sensitive data, specifically addressing information commonly linked to younger users.

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] We laud the efforts to adopt amendments that require the Department of Education to develop model programs for educating students regarding online safety while using the internet.

---

[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.

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, this bill presents the following concerns.

HB 4700's provisions regarding liability for data collection and age verification will not achieve the bill's stated objectives.

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.[5] 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 parental consent proposals that would require the additional collection of user data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.[6]

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.

Additionally, it is unclear what impact users' employment of virtual private networks (VPNs)[8] and other mechanisms to avoid location-specification age verification requirements could have on organizations' liability under this bill.

---

[5] 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.
[6] Colleen McClain, *How americans view data privacy*, Pew Research Center: Internet, Science & Tech (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[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.
[8] 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/.

This bill may result in shutting down services for all users under 18. Restricting access to the internet for teens restricts their First Amendment right to access information, including access to supportive communities that may not be accessible forums in their 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 between 14 and 17 could face a similar fate as HB 4700 would implement more complex vetting requirements tied to parental consent for users under 18.

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 or guardian" is, in fact, a minor's legal parent or guardian, especially through a means such as "call to consent" or via facsimile. It is unclear how one would verify whether the caller is the parent or guardian and how liability might apply to callers who misrepresent their identity. 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 that a "parent or guardian" 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 platform." 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 South Carolina or is not a resident of the state creates significant confusion for consumers and businesses.

The hyperconnected nature of social media has led many to allege that online services may be negatively impacting teenagers' mental health. However, some researchers argue that this theory is not well supported by existing evidence and repeats a "moral panic" argument frequently associated with new technologies and new modes of communication. Instead, social media effects are nuanced,[9] small at best, reciprocal over time, and gender-specific. Additionally, a study conducted by researchers from Columbia University, the University of Rochester, the University of Oxford, and the University of Cambridge found that there is no evidence that associations between adolescents' digital technology engagement and mental health problems have increased.[10] Particularly, the study shows that depression's relation to

[9] Amy Orben *et al.*, *Social Media's enduring effect on adolescent life satisfaction*, PNAS (May 6, 2019), https://www.pnas.org/doi/10.1073/pnas.1902058116.
[10] Amy Orben, Andrew K. Przybylski, Matti Vuorre, *There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased*, Sage Journals (May 3, 2021), https://journals.sagepub.com/doi/10.1177/2167702621994549.

both TV and social media use was practically zero. The researchers also acknowledged that it is possible, for example, that as a given technology becomes adopted by most individuals in a group, even individuals who do not use that technology could become indirectly affected by it, either through its impacts on peers or by them being deprived of a novel communication platform in which social life now takes place.

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.[11] After 25 years, age authentication still remains a vexing technical and social challenge.[12] Ohio and Arkansas recently enacted legislation that would implement online parental consent and age verification 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. The fate of a similar law in Utah is also in jeopardy as it is also facing legal challenges.[13] 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.

As South Carolina lawmakers consider several frameworks intended to address online safety, CCIA cautions against proposals that carry other significant pitfalls.

CCIA similarly cautions against pursuing laws mirroring California's 2022 "Age-Appropriate Design Code" (AADC), such as HB 4482. Requirements proposed under HB 4482 would be difficult to operationalize at scale and allow businesses to come into compliance given the bill's vague definitions. For example, HB 4482 would require businesses to provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using "clear language suited to the age of children likely to access that online service, product, or feature". The definition of "clear language suited to the age of children likely to access online services" is not defined and leaves room for significant subjective interpretation. If a child is defined as anyone under 18, one could expect a wide variation of reading comprehension skills across such a wide age group — a 17-year-old would presumably have better reading comprehension skills than that of a 5-year-old. Without "clear language" being defined, the bill would be difficult to comply with.

Additionally, the definition of "best interests of a child" is incredibly vague and impossible to operationalize at scale, creating moving goalposts for compliance. The benefit of a dynamic marketplace is that online businesses can tailor their services and products to what is most relevant and useful to their specific audience. Private online businesses will not be able to

[11] *Reno v. ACLU*, 521 U.S. 844 (1997).
[12] 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.
[13] *NetChoice, LLC v. Griffin* (W.D. Ark. 5:23-cv-05105); *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047); *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).

coherently or consistently make diagnostic assessments of users, including what could be "physically, financially, or emotionally" harmful to them. Humans in general, especially children, have very nuanced opinions surrounding what may be harmful to them. The diverse lived experiences of children, teens, and adults vary significantly, leaving businesses without a comprehensive roadmap to navigate each user's unique perspective. Determining the optimal solutions for the well-being of each and every young individual engaging with an online platform poses a serious feasibility challenge.

While HB 4482 diverges from HB 4700 by not mandating covered businesses to utilize age verification methods explicitly, it is likely that under HB 4482, age estimation would effectively amount to age verification to achieve compliance and avoid the proposed penalties for violations. Current commercially available facial recognition and other mechanisms that provide age estimation cannot sufficiently accomplish what lawmakers are expecting.[14] The AADC purports not to require age verification, but the definitions and policy itself are so vague that sites will have no choice but to implement some kind of age verification technology to achieve compliance, and unfortunately, HB 4482's approach includes these same pitfalls. Such verification requirements then raise questions about potential conflicts with data minimization principles and other consumer data privacy protection measures. Finally, it is worth noting that the California AADC is facing a legal challenge based on Constitutional concerns,[15] in addition to the aforementioned challenges in Arkansas, Ohio, and Utah.

Businesses operating online depend on clear regulatory certainty across jurisdictions nationwide.

Existing U.S. law provides websites and online businesses with legal and regulatory certainty that they will not be held liable for third-party content and conduct. By limiting the liability of digital services for misconduct by third-party users, U.S. law has created a robust internet ecosystem where commerce, innovation, and free expression thrive — all while enabling providers to take creative and aggressive steps to fight online abuse. Ambiguous and inconsistent regulation at the state level would undermine this business certainty and deter new entrants, harming competition and consumers.

Additionally, research suggests that aggressive regulations, bills, and enforcement actions targeting tech would increase operating costs for regulated U.S. companies, reducing their market value and harming their shareholders. State and local government employee pension plans are leading shareholders in companies that would be targeted by such anti-tech policies, jeopardizing the retirement benefits of 27.9 million pension plan members nationwide, including teachers, firefighters, nurses, and police.[16]

* * * * *

[14] Berin Szóka, *Comments of TechFreedom In the Matter of Children's Online Privacy Protection Rule Proposed Parental Consent Method; Application of the ESRB Group for Approval of Parental Consent Method*, TechFreedom (Aug. 21, 2023), https://techfreedom.org/wp-content/uploads/2023/08/Childrens-Online-Privacy-Protection-Rule-Proposed-Parental-Consent-Method.pdf.

[15] *NetChoice, LLC v. Bonta* (N.D. Cal. 5:22-cv-08861).

[16] *The cost of tech regulatory bills to state and local pension plans – state by state aggregates*, CCIA Research Center (Nov. 1, 2022), https://research.ccianet.org/stats/cost-of-tech-regulation-bills-state-map/.

While we share the concerns of the sponsor and the Committee regarding the safety of young people online, we encourage lawmakers 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 the Legislature considers proposals related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association