January 16, 2024

House Committee on Judiciary
Room 407, House Office Building
402 South Monroe Street
Tallahassee, FL 32399-1300

Re: HB 1 - "Social Media Use for Minors" (Oppose)

Dear Chair Gregory and Members of the House Committee on Judiciary:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 1 in advance of the House Committee on Judiciary hearing on January 17, 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. Such a privacy law should incorporate safeguards for sensitive data, specifically addressing information commonly linked to younger users. Last year, Florida passed SB 262, the "Digital Bill of Rights" which includes privacy protections, specifically those pertaining to minors.

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] Florida has already taken important steps to adopt such an approach – just last year, the legislature passed SB 52, which requires training for online safety and social media. CCIA recommends allowing this law to have an opportunity to work by training students, parents, and teachers on online safety across the state.

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 expressly

[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.

illegal cannot be suppressed solely to prevent young online users from accessing 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.

1. HB 1's provisions regarding liability for data collection and age verification will not achieve the bill's stated objectives.

HB 1 would hold covered social media companies liable for failing to perform age verification but also requires a social media company to dispose of any 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 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. For instance, compliance with the bill would force a covered entity to gather location data about every user so that they can provide helpful resources based on their zip-code. 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 the additional collection data; around 89% of Americans are very or somewhat concerned about social media platforms knowing personal information about kids.[7]

Further, no "Reasonable age verification method" currently exists. Any "commercially reasonable method" used by the government carries serious privacy and security concerns for users and should not be mandated. Notably, the Commission Nationale de l'Informatique et des Libertés (CNIL) analyzed several existing online age verification technologies 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.[8] Though the intention to keep kids

[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] 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/.
[8] *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.

safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people.

2. This bill may result in shutting down services for all users under 18. Restricting access to the internet for children 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 15 would face a similar fate as HB 1 would prohibit a minor who is younger than 16 years of age from creating a new account on the social media platform. HB 1 would also require a social media platform to terminate any account that is reasonably known to be held by a user under 16 years of age unless they dispute the termination by verifying their age within 90 days. Further, it is unclear how a social media platform is expected to manage requests to terminate an existing account if a parent makes such a request but the user has requested to maintain the status of their account.

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.

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 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.

[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.

3. Age estimation and verification 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] California and Arkansas 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.[13] The fate of similar laws in Ohio and Utah is also in jeopardy as they are also facing legal challenges.[14] 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. The Florida House of Representatives Staff analysis[15] acknowledges these other legal challenges and the likely constitutional issues that this bill presents, including the First Amendment right to freedom of speech.

4. HB 1's disclosure and disclaimer requirements raise additional legal questions and may introduce other risks for social media platform users.

HB 1 introduces additional First Amendment concerns regarding compelled speech, as the bill would require a social media platform, if it offers services to users under 18 years of age, to post a disclaimer stating "This application may be harmful to your mental health and may use design features that have addictive qualities or present unverified information or that may be manipulated by [insert platform name] or others for your viewing" in addition to information about the platforms content moderation policies. First, as previously discussed, there is not any confirmed *causal link* between mental health risk and social media use for users and requiring a social media platform to assert as much is not founded in currently available scientific research. Second, in a recent ruling in *NetChoice v. Bonta*[16] the court questioned the constitutionality of such compelled disclosures surrounding design features. Specifically, the court found California's argument unpersuasive, that requiring businesses to affirmatively disclose information to users and the government is *unrelated* to speech.

Separate from the legal concerns, such disclosures also introduce risk associated with potential exploitation by bad actors. Rather than protecting consumers from potentially harmful content, these disclosures might have the adverse unintended consequence of giving nefarious foreign agents, purveyors of harmful content, and other bad actors a playbook for circumventing digital services' policies.

Finally, the disclosure requirements introduce ambiguity, particularly those surrounding whether the social media platform allows "manipulated content". It is unclear whether this would include basic functions such as image cropping – as such, this overly broad requirement could ultimately result in a degraded experience for users.

---

[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. Bonta* (N.D. Cal. 5:22-cv-08861); *NetChoice, LLC v. Griffin* (W.D. Ark. 5:23-cv-05105).
[14] *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *NetChoice, LLC v. Yost* (S.D. Ohio 2:24-cv-00047).
[15] Florida House of Representatives Staff Analysis of FL HB 1, https://flsenate.gov/Session/Bill/2024/1/Analyses/h0001.RRS.PDF (Jan. 9, 2024).
[16] *See supra* note 13.

5. 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.[17]

* * * * *

While we share the concerns of the sponsor and the Committee regarding the safety of young people online, we encourage Committee members 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

[17] *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/.