February 21, 2025

Vermont Legislature
115 State St
Drawer 33
Montpelier, VT 05633

Re: S. 69 – "Vermont Age-Appropriate Design Code Act" (Oppose)

Dear Chair Harrison, Vice Chair Plunkett, and members of the Senate Institutions Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose S. 69. CCIA opposed H. 121 last year and appreciated Governor Phil Scott's decision to veto the measure until a court decision had been reached in California regarding a similar measure which was blocked over constitutional concerns.[1] As that litigation is still ongoing, this proposal remains premature. Nonetheless, we are grateful for the opportunity to share our concerns with the Senate Institutions Committee.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[2] Proposed regulations on the interstate provision of digital services can therefore significantly impact CCIA members. CCIA and its members have a shared interest in protecting children and giving parents and adults simple but effective tools to provide a safe online environment for their families.

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and parental tools to individually tailor younger users' online use to their 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 allow parents to block specific sites entirely.[3] This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.[4]

However, 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.[5] While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

---

[1] Press Release, Action Taken by Governor Phil Scott on Legislation (June 13, 2024), https://governor.vermont.gov/press-release/action-taken-governor-phil-scott-legislation-june-13-2024.
[2] 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.
[3] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/.
[4] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.
[5] *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212–14 (1975). *See also FCC v. Pacifica Found.* 438 U.S. 726, 749–50 (1978); *Pinkus v. United States*, 436 U.S. 293, 296–98 (1978).

Requirements under S. 69 are not administrable or well defined, creating serious compliance questions for both businesses and users.

S. 69 would create many vaguely defined obligations for businesses, leaving them unable to know whether they are violating the law. For instance, the law covers businesses "whose online products, services, or features are reasonably likely to be accessed by a minor." Websites are determined to be "reasonably likely to be accessed by a minor" based on indefinite criteria such as "competent and reliable evidence regarding audience composition," with no indication of what might constitute such evidence. Moreover, any business that "knew or should have known that at least two percent of the audience of the online service, product, or feature includes minors two through 17 years of age" is subject to this law. There is no definitive criteria for determining whether a business "should have known" such percentages, and this provision is broad enough to encompass nearly every business with a public-facing website.

Further, the "minimum duty of care" standard is vague and problematic. Requiring action against ill-defined categories of harm such as "reasonably foreseeable emotional distress" and "compulsive use" fails to provide services with the legal clarity they need to comply. It incentivizes overbroad filtering or restrictions on content and features, limiting important access to information, the ability to build community, and freedom of expression. Without some certainty as to what types of designs would lead to significant penalties, covered businesses will likely err on the side of caution. This will make it more difficult for users to access new or innovative services.

Additionally, the terms "covered minor" and "known adult" extend not only to consumers a business knows to be minors or adults, but also to those "label[ed] as a minor pursuant to age assurance methods in rules adopted by the Attorney General," with no guidance as to what assurance methods the Attorney General might use. These highly subjective and overinclusive definitions make it difficult for businesses to ascertain, let alone comply with, their obligations. CCIA recommends using narrower and more objective criteria to define which businesses are covered and what legal obligations they could face, and basing businesses' obligations on their actual knowledge of user ages, rather than what they "should have known."

S. 69 would force companies to collect more data about minors to ensure compliance, jeopardizing their privacy.

The bill's vague and overbroad compliance burdens incentivize covered businesses to increase their collection of sensitive data about minors and their parents for age verification purposes. To ensure compliance, businesses would need to *determine the age of all users* to ensure that they can adhere to the regulations regarding minors. This would in turn require using invasive age verification methods that force businesses to collect sensitive personal identifying information about their users.[6] Although the bill does not directly require age verification, the definitions and policy itself are so vague that sites will have no choice but to implement some

[6] 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.

form of age verification technology to ensure compliance. S. 69 will therefore require the collection of detailed personal information about children and adults that will create massive data pools, which criminals will attempt to target for purposes of identity theft.

To avoid restricting teens' access to information, S. 69 should regulate users under 13 rather than 18 in accordance with established practices.

S. 69 defines a minor as anyone under 18. Due to the nuanced ways in which children under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, if a 16-year-old is conducting research for a school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. We would suggest changing the definition of "minor" to a user under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard. This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources.

If enacted, S. 69 may result in denying services to all users under 18. Limiting access to the internet for children curtails their First Amendment right to information accessibility, including access to supportive communities that may not be open-discussion forums in their physical location.

The lack of narrowly tailored definitions, as discussed above, could incentivize businesses to simply prohibit minors from using digital services rather than face potential legal action and hefty fines for non-compliance. The First Amendment, including the right to access information, is applicable to teens.[7] Moreover, requiring businesses to deny access to social networking sites or other online resources may also unintentionally restrict children's ability to access and connect with like-minded individuals and communities. For example, children of certain minority groups may not live in an area where they can easily connect with others that represent and relate to their own unique experiences, so an online central meeting place where kids can share their experiences and find support can have positive impacts.[8]

The connected nature of social media has led some to allege that online services may be negatively impacting teenagers' mental health. However, researchers explain that this theory is not well supported by existing evidence and repeats a 'moral panic' argument frequently associated with new technologies and modes of communication. Instead, social media effects are nuanced,[9] individualized, reciprocal over time, and gender-specific. A study conducted by researchers from several leading universities found no evidence that associations between adolescents' digital technology engagement and mental health problems have increased.[10]

---

[7] *See, e.g.*, *Reno v. ACLU*, 521 U.S. 844, 874-75 (1997).
[8] *The Importance of Belonging: Developmental Context of Adolescence*, Boston Children's Hospital Digital Wellness Lab (Oct. 2024), https://digitalwellnesslab.org/research-briefs/young-peoples-sense-of-belonging-online/.
[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 et al., *There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased*, Sage J. (May 3, 2021), https://journals.sagepub.com/doi/10.1177/2167702621994549.

Particularly, the study shows that depression has virtually no causal relation to TV or social media.

As explained above, CCIA believes that an alternative to solving these complex issues is to work with businesses to continue their ongoing private efforts to implement mechanisms such as daily time limits or child-safe searching so that parents can have control over their own child's social media use.

Currently available tools to conduct age determination are imperfect in estimating users' ages.

There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy[11] and small business sustainability.[12] A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains more information regarding guiding principles for age assurance and how digital services have used such principles to develop best practices.[13] The report found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification or assurance methods, and that "[h]ighly accurate age assurance methods may depend on collection of new personal data such as facial imagery or government-issued ID."[14]

Additionally, age verification or determination software does not process all populations with equal accuracy. The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[15] The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA encourages lawmakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

S. 69's vague standards and obligations are likely to lock adult users out from valuable information and services they depend upon if they're unable to verify their age. This is because no age verification or estimation mechanism is 100% accurate, and there will always be false positives that impact adult users.

[11] Kate Ruane, *CDT Files Brief in* NetChoice v. Bonta *Highlighting Age Verification Technology Risks* (Feb. 10, 2025), https://cdt.org/insights/cdt-files-brief-in-netchoice-v-bonta-highlighting-age-verification-technology-risks/.
[12] Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf.
[13] *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[14] *Id.* at 10.
[15] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* Nat'l Inst. Standards & Tech. (May 30, 2024), https://doi.org/10.6028/NIST.IR.8525.

S. 69's penalties for violations pose significant questions regarding compliance.

In order to achieve meaningful children's safety protections, it is imperative for businesses to have a roadmap of how to properly comply and avoid unintentional violations.[16] This measure provides broad strokes of *what* is expected of businesses but does not portend *how* businesses may achieve those objectives. CCIA cautions against conflating concepts regarding estimating the age of users.[17] For example, when a website asks a user to make a self-attestation of their age, such as on a website for alcohol products, the owner of that website is not held liable if that user chooses to mischaracterize their identity. Similarly, the age-estimation mechanisms outlined in S. 69 are not fully capable of determining the age of a given user, and therefore, if a business relies upon one of those methods, they may expose themselves to liability if they do not accurately determine who is under the age of 18.

Related proposals with similar requirements for online businesses are currently being litigated in several different 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.[18] After 25 years, age authentication still remains a vexing technical and social challenge.[19]

Recent state legislation that would implement online age verification or estimation measures is currently facing numerous constitutional challenges, and numerous federal judges have placed laws on hold until these challenges can be fully reviewed, including in Arkansas, California, Mississippi, Ohio, Tennessee, Texas, and Utah.[20] CCIA anticipates that these forthcoming rulings may clarify which age determination requirements are Constitutionally permissible. CCIA therefore 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 Vermont taxpayers.[21]

* * * * *

[16] Digital Trust & Safety Partnership, *Age Assurance: Guiding Principles and Best Practices* (Sept. 2023), https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.
[17] Khara Boender, *Children and Social Media: Differences and Dynamics Surrounding Age Attestation, Estimation, and Verification*, Disruptive Competition Project (May 10, 2023), https://www.project-disco.org/privacy/children-and-social-media-differences-and-dynamics-surrounding-age-attestation-estimation-and-verification.
[18] *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).
[19] Jackie Snow, *Why Age Verification Is So Difficult for Websites*, Wall St. J. (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.
[20] *See, e.g.*, *NetChoice v. Bonta*, No. 24-cv-07885, 2025 WL 28610 (N.D. Cal. Jan. 2, 2025); *NetChoice v. Bonta*, No. 22-cv-08861, 2024 WL 5264045 (N.D. Cal. Dec. 31, 2024); *NetChoice, LLC v. Reyes*, No. 23-cv-00911, 2024 WL 4135626 (D. Utah Sept. 10, 2024); *NetChoice, LLC v. Fitch*, No. 24-cv-00170, 2024 WL 3276409 (S.D. Miss. July 1, 2024); *NetChoice, LLC v. Yost*, 716 F. Supp. 3d 539 (S.D. Ohio 2024); *NetChoice, LLC v. Griffin*, No. 23-cv-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023); *Comput. & Commc'ns Indus. Ass'n et al. v. Paxton*, No. 24-cv-00849, 2024 WL 4051786 (W.D. Tex. Aug. 30, 2024).
[21] Gov. Scott clearly explained this in his veto letter of H. 121. *See supra* note 1 ("While this is an important goal we can all support, similar legislation in California has already been stopped by the courts for likely First Amendment violations. We should await the decision in that case to craft a bill that addresses known legal pitfalls before charging ahead with policy likely to trigger high risk and expensive lawsuits. Vermonters will already be on the hook for expensive litigation . . . and should not have to pay for additional significant litigation already being fought by California.").

While we share the concerns regarding the safety of young people online and the importance of data privacy, we encourage you to resist advancing legislation that poses significant compliance and constitutional concerns.

We appreciate your consideration of these comments and welcome opportunities to provide additional feedback on this and other technology policy matters.

Sincerely,

Megan Stokes
State Policy Director
Computer & Communications Industry Association