April 5, 2024

House Committee on Commerce and Economic Development
Attn: Jon Gray, Legislative Counsel
115 State Street
Montpelier, VT 05633

RE: S. 289 - An Act relating to age-appropriate design code (Oppose)

Dear Chair Marcotte and Members of the Commerce and Economic Development Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose S. 289, an act relating to age-appropriate design code.

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, something that the Committee has done a tremendous amount of work on.

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]

CCIA appreciates the Committee's consideration of our comments, and has outlined our concerns with the current language of S. 289 below.

[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/.

As drafted, S. 289 would create several conflicts with the comprehensive data privacy proposal being advanced in Vermont.

CCIA appreciates the extensive work the Committee has done in the past few years to put forward comprehensive data privacy legislation (H. 121), with the goal of protecting Vermont residents' data at the core of that effort. As the Committee considers S. 289 it is important to point out the several ways in which this legislation conflicts with H. 121 both in principle, as well as in the requirements each bill would create.

First and foremost, if passed, S. 289 would almost certainly result in companies needing to collect significant amounts of additional personal information about Vermont residents in order to achieve compliance. Covered businesses would need to determine a user's age and how age-specific requirements under the bill should be applied, which would necessitate the collection of sensitive information like personal identifiers and geolocation data. Counter to S. 289's intended goals, this would paradoxically force companies to collect a higher volume of data on children.[4] Businesses may be forced to collect personal information they don't want to collect and consumers don't want to give, and that data collection creates extra privacy and security risks for everyone while undermining proposed protections under H. 121. 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.[5] Though the intention to keep kids safe online is commendable, S. 289 is counterproductive to that initiative by requiring more data collection about all internet users, including young people.

Furthermore, S. 289 and H. 121 outline conflicting responsibilities and requirements for businesses, specifically when it pertains to data protection impact assessments (DPIAs) and duties of care. The two bills have different standards for compliance with their "duty of care" requirements. H. 121 would impose a duty of care on businesses that offer services or products to consumers whom the business actually knows or willfully disregards are under the age of 18, while S. 289 would establish a duty of care standard for any business that processes a "minor consumer's data in any capacity". These conflicting standards would confuse businesses and obfuscate any meaningful roadmap for compliance. Additionally, H. 121 would require DPIAs for processing activities that present a "heightened risk of harm", as well as for businesses who offer products or services to a consumer whom the business actually knows or willfully disregards is under the age of 18, while S. 289 omits DPIAs entirely. This conflict

[4] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard.
[5] *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.

would only serve to confuse businesses covered by both bills, leaving them in doubt as to how they would demonstrate compliance with the standards set out in each proposal.

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.[6] After 25 years, age authentication still remains a vexing technical and social challenge.[7] 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 these laws on hold until these challenges can be fully reviewed.[8] The fate of a similar law in Utah is also in jeopardy as it is also facing a legal challenge.[9] CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary in these ongoing challenges before burdening businesses with legislation that risks being invalidated or passing on expensive litigation costs to taxpayers.

The bill lacks narrowly tailored definitions.

As currently written, the bill defines a child 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 suggest changing the definition of "child" 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.

The bill would also require businesses to provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using "language suited to the age of a minor consumer reasonably likely to access that online service, product, or feature." This 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

[6] *Reno v. ACLU*, 521 U.S. 844 (1997).
[7] 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.
[8] *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).
[9] *NetChoice, LLC v. Reyes* (D. Utah 2:23-cv-00911); *Zoulek et al. v. Hass & Reyes* (D. Utah 2:24-cv-00031).

skills than that of a 13-year-old. Without this standard being defined, the bill would be difficult to comply with.

Finally, while the definition of "low friction variable reward" does include a handful of examples, the list provided is not exhaustive and could unintentionally scope in items like push notifications for potential fraud or security flags, or other consumer-desired information such as shipping updates. CCIA suggests that the definition be amended to exempt other useful and beneficial functions, such as for personalization, or to support consumer needs.

S. 289's provisions regarding the "profiling" of a child and the enforcement of 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.[10] This measure provides broad strokes of *what* is expected of businesses but does not portend *how* businesses may achieve those objectives. Instead, businesses may be allowed to profile a child under certain circumstances. CCIA interprets this as necessitating businesses to distinguish users aged below and above 18. We recommend providing clarity on the procedures businesses should follow to determine the age of users online, specifically when "profiling" them as children. Without a proper mechanism in place, businesses may encounter challenges in accurately determining the age of each individual user, potentially resulting in unintended violations for which the business may be held liable.

CCIA cautions against conflating concepts regarding "profiling" or estimating the age of users.[11] 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. Similar self-attestation measures are currently in place for social media platforms and other digital services, and the burden is on the consumer to be forthcoming and honest about the age and birthdate they enter. This, however, would change under S. 289 — if online services were to rely on self-attestation for estimates but then in turn be held liable for mischaracterizations, this would unreasonably treat the business as the bad actor.

To achieve compliance and avoid the proposed penalties for violations, it is likely that "profiling" or age estimation would effectively amount to age verification. Current commercially available facial recognition and other mechanisms that provide age estimation cannot

[10] 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.
[11] 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.

sufficiently accomplish what lawmakers are expecting.[12] 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, S. 289's approach includes these same pitfalls.

S. 289 risks 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 First Amendment, including the right to access information, is applicable to all Americans, including teens. Vague restrictions on protected speech cannot be justified in the name of "protecting" minor users online, nor is a state legislative body the arbiter of what information is suitable for younger users to access. Moreover, 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, children of racial or other minority groups may not live in an area where they can easily connect with others that represent and relate to their own unique experiences. An online central meeting place where kids can share their experiences and find support can have positive impacts.

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. This particularly applies to new small businesses that tend to operate with more limited resources and could be constrained by costs associated with compliance. While larger companies may be able to more easily absorb such costs, it could disproportionately prevent new smaller start-ups from entering the market.

Further, careful consideration of what constitutes best practice should consider inputs from practitioners and relevant stakeholders. Online businesses are already taking steps to ensure a

[12] 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.

safer and more trustworthy internet — recently, leading online businesses announced[13] that they have been voluntarily participating in the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices and recently reported on the efforts to implement these commitments.[14] We urge lawmakers to study both the benefits and drawbacks of teen safety and privacy requirements and to engage with practitioners and stakeholders to support the ongoing development of practicable solutions.

* * * * *

While we share the concerns 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,

Alex Spyropoulos
Regional Policy Manager, Northeast
Computer & Communications Industry Association

[13] Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), https://www.axios.com/techgiants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html.
[14] *See, e.g.*, DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* (July 2022), https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf (Appendix III: Links to Publicly Available Company Resources), at 37.