May 30, 2024

The Office of Honorable Phil Scott, Governor of Vermont
109 State Street, Pavilion
Montpelier, VT 05609

RE: H.121 - An Act relating to enhancing consumer privacy and the age-appropriate design code (Veto Request)

Dear Governor Scott,

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto on H.121.

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.

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 shares Vermont's goal of promoting online safety, particularly for minors, but Section 7 of H.121 raises several constitutional and compliance issues that warrant significant concern.

Furthermore, CCIA strongly supports the protection of consumer data and understands that Vermont residents are rightfully concerned about the proper safeguarding of their data. We are concerned, however, with several aspects of H. 121 which differ from other existing state privacy laws, which will impact businesses of all sizes. We are particularly concerned about the inclusion of a private right of action, the definition of "sale", the language included around targeted advertising, and data minimization principles.

---

[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/.

Pertaining to Section 7 of H. 121 - Age Appropriate Design Code

The bill lacks narrowly tailored definitions.

Section 7 of H. 121 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.

Furthermore, 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 helpful mechanisms 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.

Section 7 of H. 121's provisions regarding the "minimum duty of care" of a minor 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.[4] 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.[5] 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 Section 7 of H. 121 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 be opening themselves up to liability under the bill if they do not accurately determine who is under the age of 18.

Section 7 of H. 121 imposes several obligations upon businesses' use of consumers' data but also provides specific requirements and restrictions regarding consumers under the age of 18.

---

[4] 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.

[5] 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.

To comply, however, businesses would be required to *determine the age of all users to* ensure that they can adhere to the relevant regulations if the consumer was a minor or not. To avoid the significant penalties provided under Section 7 of H. 121 , businesses would have no alternative than to use age verification mechanisms in order to avoid the risk of failing to treat users accordingly under the bill. Current commercially available facial recognition and other mechanisms that provide age estimation cannot sufficiently accomplish what lawmakers are expecting.[6] 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, H. 121's approach includes these same pitfalls. H. 121 will 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.

Further, the "minimum duty of care" establishes a vague and problematic standard, prohibiting businesses from using minors' personal data or design features that would "benefit the [business] to the detriment of a child". This is an extremely vague standard, both in terms of what it means to "benefit the business" and to do so "to the detriment of a child." What is more, the standard is in conflict with other parts of the bill, such as § 2420 which requires data controllers that know or consciously avoid knowing its users are minors to use "reasonable care to avoid heightened risks of harm." Requiring action against ill-defined categories of harm fails to provide services with the legal clarity they need to take action. It incentives over broad filtering or restrictions on content and features – limiting important access to information, the ability to build community, freedom of expression, and creativity. Without some level of certainty as to what types of designs would give rise to a lawsuit with significant penalties, platforms will err on the side of caution. This will make it more difficult for our users to access new or innovative services.

Section 7 of H. 121 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 individuals, 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

[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.

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. H.121's vague standards and obligations is 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 mechanism is 100% accurate, and there will always be false positives that impact adult users.

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.[7] After 25 years, age authentication still remains a vexing technical and social challenge.[8] 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.[9] The fate of a similar law in Utah is also in jeopardy as it is also facing a legal challenge.[10] CCIA recommends that Vermont 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.

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.

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

Pertaining to Section 1 of H. 121

Including a private right of action subjects businesses to frivolous claims and could overwhelm Vermont's judicial system.

§ 2424 of Section 1 of H. 121 permits consumers to bring legal action against businesses that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Vermont's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual consumers in Vermont, disproportionately impacting smaller businesses and startups across the state. Further, every state that has established a comprehensive consumer data privacy law – now over 15 states – has opted to invest enforcement authority with their respective state attorney general. This allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

Several aspects of Section 1 of H. 121 differ from other existing state privacy laws and as such will cause difficulty for businesses of all sizes operating in Vermont.

In the absence of a federal privacy framework, interoperability between state privacy laws is crucial to avoid placing a difficult, confusing, and costly compliance burden on businesses. Several aspects of H. 121 differ from other existing state privacy laws and therefore will cause difficulty for businesses of all sizes operating in Vermont.

Beginning with the definition of "sale of personal data", which is overly broad and would include any exchange of consumer data for any "commercial purpose". This differs from the definitions included in any other state privacy law, which are typically focused on monetary or other valuable considerations. This definition would have a significant impact on businesses who make a sizable portion of their revenue from online sales, including small businesses, who rely on third-parties for basic tasks, like marketing, analytics, and cloud storage. These services often require some exchange of personal data to function effectively. Because these businesses exchange consumer data with these services for a commercial purpose, basic business operations could constitute a "sale", forcing small businesses to completely rework their day-to-day operations and increasing administrative costs. In addition, if an extensive array of business activities is classified as "sales", businesses would need to provide opt-outs and manage consent far more frequently.

Furthermore, language included around the definition of "targeted advertising" that would exclude advertisements based on activities within a controller's own "commonly branded websites or applications". No other state includes "commonly branded" in their privacy law,

and in doing so, targeted advertising to a company's customers by affiliates could be restricted even though a consumer expected such advertising.

Finally, the inclusion of a confusing data minimization principle in H. 121 would leave businesses in an ambiguous position, as each business would have to determine what purposes are reasonably necessary and compatible with a disclosed purpose and risk violating the law. Under such a standard, it would be possible that basic advertising practices and using data to improve products could be impermissible. This would not only harm businesses in Vermont, but would hinder consumers' ability to access improved services.

* * * * *

While we share the concerns regarding the safety of young people online and the importance of data privacy, we encourage you to resist signing legislation that poses significant compliance and constitutional concerns and respectfully request a veto of H. 121.

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

Sincerely,

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