April 17, 2023

Senate Judiciary and Public Safety Committee
Attn: Nicole Kaplan, Committee Administrator
Minnesota Senate Bldg.
St. Paul, MN 55155

RE: SF 2810 - "Minnesota Age-Appropriate Design Code Act" (Oppose)

Dear Chair Latz and Members of the Senate Judiciary and Public Safety Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SF 2810.

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. Recent sessions have seen an increasing volume of state legislation related to the regulation of digital services. While recognizing that policymakers are appropriately interested in the digital services that make a growing contribution to the U.S. economy, these bills require study, as they may raise constitutional concerns, conflict with federal law, and risk impeding digital services companies in their efforts to restrict inappropriate or dangerous content on their platforms.[2]

CCIA strongly believes children deserve an enhanced level of security and privacy online. Currently, there are a number of efforts among our members to incorporate protective design features into their websites and platforms.[3] CCIA's members have been leading the effort in raising the standard for teen safety and privacy across our industry by creating new features, settings, parental tools, and protections that are age-appropriate and tailored to the differing developmental needs of young people.

While CCIA strongly supports the overall goal of keeping children safe online, there are many concerns we would like to raise about the policies this bill would implement.

1. 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.

[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] Taylor Barkley, Aubrey Kirchhoff, and Will Rinehart, *5 things parents and lawmakers need to know about regulating and banning social media*, The CGO (Mar. 7, 2023), https://www.thecgo.org/benchmark/5-things-parents-and-lawmakers-need-to-know-about-regulating-and-banning-social-media/?utm_source=substack&utm_medium=email.

[3] 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/.

The definition of "likely to be accessed by children" is also ambiguous. CCIA recommends narrowly tailoring this definition to content intentionally targeted at or branded for children when they are using the internet.

The bill would also 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 law is difficult to comply with.

2. The bill does not provide how a user's age will be estimated and how penalties for those who do not abide by the law will be enforced.

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. This measure provides broad strokes of *what* is expected of businesses but does not portend *how* businesses may achieve those objectives. Instead, businesses are expected to estimate ages to a "reasonable level of certainty". CCIA suggests clarifying how businesses are expected to estimate the age of users online. Without a proper mechanism in place, it is difficult for businesses to discern the age of every individual user which could lead to unintended violations.

CCIA cautions against conflating concepts regarding estimating the age of users. 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 birth dates they enter. This, however, would change under SF 2810 – if online services were to rely on self-attestation for estimates but then in-turn be held liable for mischaracterizations, this would present severe culpability concerns and treat the business as the bad actor. Further, it is unclear what impact the use of VPNs and similar mechanisms to evade age verification by users could have on organizations' liability under this bill.

To achieve compliance and avoid the proposed penalties for violations, it is likely that age estimation would amount to age verification. Such verification requirements then raise questions about potential conflicts with data minimization principles and other consumer data privacy protection measures. CCIA is concerned that businesses may be forced to collect age verification data, which 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. This forced data collection would include collecting highly sensitive personal information about children, including collecting and storing their geolocation to ensure they do not reside outside of the state when confirming that they are of age to be using these services. 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,

[4] 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.

it may place businesses in an untenable position of picking which state's law to comply with, and which to violate.[5]

When the Communications Decency Act was passed, there was an effort to sort the online population into kids and adults for different regulatory treatment. That requirement was struck down as unconstitutional because of the infeasibility. Yet, after 25 years, age authentication still remains a vexing technical and social challenge.[6] 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.

3. Restricting access to the internet for children also restricts their access to supportive communities that may not be accessible forums in their physical location.

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.

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,[7] small at best, reciprocal over time, and gender-specific. Teens themselves also paint a nuanced picture of the effects of social media. It is one in which majorities credit these platforms[8] with deepening connections and providing a support network when they need it. In a recent survey, 80% of teens say that what they see on social media makes them feel more connected to what's going on in their friends' lives, while 71% say it makes them feel like they have a place where they can show their creative side. Additionally, 67% also say these platforms make them feel as if they have people who can support them through tough times.

4. 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.

---

[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] 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.

[7] 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.

[8] Monica Anderson *et al.*, *Connection, creativity and drama: Teen life on social media in 2022,* Pew Research Center: Internet, Science & Tech (Nov. 17, 2022), https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/..

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 involve conversations with practitioners and relevant stakeholders. Online businesses are already taking steps to ensure a safer and more trustworthy internet — recently, leading online businesses announced[9] 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.[10] 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.

5. In the United Kingdom, the Age Appropriate Design Code is not an enforceable law, but is regulatory guidance for ensuring compliance with the U.K. Data Protection Act.

The Age Appropriate Design Code of the United Kingdom is not a law, but regulatory guidance, rooted in a UN Convention to which the United States does not belong. It is possible for a business to comply with U.K. law while *not* following the U.K. AADC. In fact, the U.K. Data Protection Act ("DPA") explicitly states that a *"failure by a person to act in accordance with a provision of a code issued under section 125(4) does not of itself make that person liable to legal proceedings in a court or tribunal."*[11] The code was designed by the U.K. Information Commissioner's Office to meet its obligations under the U.K. DPA to prepare a code or suggestions for safe practice.

Many proponents of the Age Appropriate Design Code in the United States claim that the U.K's internet is "still working." However, this mischaracterizes the approach taken in the U.K. United Kingdom businesses processing personal data about U.K. children are not required to implement "*age estimations*" or other requirements in this bill in order to operate. U.K. legislators avoided imposing "age verification" or similar higher thresholds upon organizations, recognizing the tension between higher accuracy and further data collection.

The U.K. also does not have the same fundamental and structural laws and rights that Americans do such as the Constitution and its First Amendment, nor does it share Americans' noted affinity for expensive civil litigation. Under U.S. law, where the bill's language would be legally enforceable, covered entities would be forced to implement *age verification* measures to avoid potential liability – even if they did not want to direct their services to children.

* * * * *

[9] 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.
[10] *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.
[11] *Age appropriate design: A code of practice for online services*, ICO (Retrieved March 2, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/

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,

Jordan Rodell
State Policy Manager
Computer & Communications Industry Association