March 25, 2025

Illinois State Senate
Senate Subcommittee on AI and Social Media
Statehouse
Springfield, IL 62706

Re: SB 50 – Illinois Age-Appropriate Design Code Act (Oppose)

Dear Senator Cunningham:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 50. 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 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.[2] 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.[3]

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

Requirements under SB 50 are not administrable or well defined, creating serious compliance questions for both businesses and users.

SB 50 would create many vague or undefined obligations for businesses, leaving them unable to know whether they are violating the law. For example, the bill requires covered entities to

[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] Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/ (last updated Feb. 19, 2025).
[3] 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/.
[4] *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).

process children's data "in a manner consistent with the best interests of children." Such a definition fails to provide covered entities with the legal clarity they need to comply, especially since acting in the "best interests of children" is defined using vague criteria such as whether a covered entity causes "reasonably foreseeable" harms and whether such an entity "knew or should have known that a significant number of users are children." Additionally, determining "whether the online product, service, or feature is designed and offered in an age-appropriate manner" is a highly subjective endeavor, as is determining whether such services, products, and features are "reasonably likely to be accessed by children."

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.

Ambiguous provisions may also incentivize 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.

SB 50's vague language effectively forces covered entities to implement the same age verification measures it purports not to require.

Although Section 45(3) states that "Nothing in this Act shall be interpreted or construed to require a covered entity to implement an age gating requirement," the vague knowledge standard noted above renders it impossible for covered entities to ensure compliance without instituting age verification. If a covered entity can be held liable even when it does not know a user's age, it can only ensure compliance by knowing the ages of all its users. SB 50's knowledge standard therefore incentivizes covered entities to collect more data about both child and adult users than they would ordinarily.

This overcollection of data carries considerable downside. There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy[5] and small business sustainability.[6] 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.[7] 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."[8]

[5] 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/.
[6] 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.
[7] *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.
[8] *Id.* at 10.

Additionally, age verification or determination software does not process all populations with equal accuracy. To avoid these pitfalls and preserve user privacy, CCIA encourages lawmakers to limit potential liability to cases where the covered entity actually knows a user's age rather than cases where it "knew or should have known" a user's age.

To avoid restricting teens' access to information, SB 50 should regulate users under 13 rather than 18 in accordance with established practices.

SB 50 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 would 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.

If enacted, SB 50 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.[9] 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.[10]

The connected nature of social media has led some to allege that online services may negatively impact 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,[11] 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.[12] As

[9] *See, e.g.*, *Reno v. ACLU*, 521 U.S. 844, 874-75 (1997).
[10] *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/.
[11] 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.
[12] 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.

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.

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.[13] After 25 years, age authentication still remains a vexing technical and social challenge.[14]

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.[15] In California, for instance, a federal judge recently issued a preliminary injunction against a state age-appropriate design code law with many similar or equivalent provisions, finding the law to be "content-based on its face"[16] and to "likely fail strict scrutiny."[17] 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 Illinois taxpayers.

A comprehensive privacy bill is the best way to protect minors online.

A better way forward is to pass a comprehensive privacy law with enhanced protections for children. A leading example is Connecticut's recently implemented privacy law, which includes enhanced protections for minors.[18] The law requires an opt-in for any collection of sensitive or precise geolocation data from known children and requires covered entities to indicate when they are collecting precise geolocation data. It gives children and their families the right to request copies of all personal data held by covered entities, and to request correction or removal of such data. The law also requires services to collect and retain the minimum amount of data necessary to provide services to known children, and bans cross-contextual behavioral advertising, including first-party targeted advertising, to known children. These measures are

[13] *See Reno*, 521 U.S. at 855-57, 862.
[14] 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.
[15] *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).
[16] Order Granting Plaintiff's Second Motion for Preliminary Injunction at 13, *NetChoice v. Bonta*, No. 22-cv-08861-BLF (N.D. Cal. Mar. 13, 2025).
[17] *Id.* at 23.
[18] Social Media Platforms, Online Services, Products or Features and Minors, Conn. Gen. Stat. § 42-528, 42-529, https://www.cga.ct.gov/2024/sup/chap_743jj.htm#sec_42-528.

concrete and specific enough that covered entities will know what actions are compliant, avoiding age assurance measures that undermine privacy for adults and children, which may reduce the likelihood of invalidation on First Amendment grounds.

* * * * *

While we share the concerns regarding the safety of young people online, 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