March 17, 2025

Florida Senate
Attn: Commerce and Tourism Committee
404 South Monroe Street
Tallahassee, FL 32399-1100

Re: SB 1438 – "Online Access to Materials Harmful to Minors" (Oppose)

Dear Chair Leek and Members of the Commerce and Tourism Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose SB 1438 in advance of the Committee on Commerce and Tourism hearing on March 17, 2025. 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.

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, this bill presents the following concerns:

The bill's provisions harm businesses operating online, who depend on clear regulatory certainty across jurisdictions nationwide, and their users.

Ambiguous and inconsistent regulation at the state or local levels undermines business certainty, creating significant confusion surrounding compliance. This type of regulatory balkanization may deter new entrants, harming competition, innovation, and consumers. Devices sold into a national market are not and cannot be designed to function differently merely because they have moved within a state's borders.

Further, SB 1438 creates significant liability concerns due to the subjective nature of what may be considered "material harmful to minors," which appears to be based on the definition of

[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/.
[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/.

"obscenity."[4] There is no systematic, objective way to differentiate obscenity from protected speech; such determinations must instead be made on a case-by-case basis, as the bill appears to acknowledge.[5] Covered entities cannot be expected to make such subjective assessments, and will inevitably engage in over-filtering to ensure compliance.

Requirements under SB 1438 are not administrable or well defined, creating serious compliance questions for businesses and users.

SB 1438 contains vague and potentially conflicting definitions that would impose significant requirements and restrictions on covered entities including manufacturers, developers, application stores, and operating system providers, and fail to make children safer.

The bill covers applications that are "likely to be accessed by children," which is defined by whether it is "reasonable to expect that an application would be accessed by children." The bill's broad duties for developers and manufacturers of covered applications include "[t]o the extent applicable and technically feasible, provide readily available features for parents to protect a user that is a child as appropriate to the risks that arise from the child's use of the developer's covered application." Several of these words do not appear elsewhere in the bill, including "applicable" and "risks." These standards are highly subjective and will be difficult to enforce with any degree of consistency. Similarly, the knowledge standard in § 501.1741(5) says "actual knowledge, through receipt of a signal regarding a user's age or otherwise." What does "otherwise" entail?

Furthermore, the safe harbor provision only applies when covered manufacturers have taken "commercially reasonable and technically feasible steps" to determine or estimate a user's age, which, like much of the bill, fails to provide businesses with the certainty they need to operate and only invites litigation over what qualifies as "reasonable" or "feasible."

To avoid restricting teens' access to information, SB 1438 should regulate users under 13 rather than 18 in accordance with established practices.

SB 1438 defines a "child" as "an individual consumer" 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.

[4] SB 1438's definition of "material harmful to minors" appears to be based on the test for "obscenity" in *Miller v. California*, 413 U.S. 15, 24 (1973).
[5] *Id.*

Age verification and parental consent requirements raise significant privacy concerns.

Every approach to age determination presents trade-offs between accuracy and privacy[6]—in addition to significant costs, especially for startups[7]—and there is no one-size-fits-all approach. Different services consider various factors, including but not limited to their user base, the service offered, risk calculation, privacy expectations, and economic feasibility. A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, contains guiding principles for age assurance and discusses how digital services have used such principles to develop best practices.[8]

The proposed bill does not meet these standards. In particular, the proposed overcollection of data about children in § 282.803(2) includes many highly invasive provisions that would make kids less safe, requiring the collection and storage of sensitive data that could be exploited. For example, the real-time data access requirement would undermine privacy and make children less safe, as developers would have access to sensitive personal information identifying an app store provider's users, including parents of their underage customers. Such excessive monitoring has been shown to negatively affect young people's mental health and development.[9]

The proposed bill suggests imposing a government-mandated requirement to verify all Florida users' ages that conflicts with data minimization principles ingrained in standard federal and international privacy and data protection compliance practices.[10] Determining a user's age and verifying parental consent inherently requires collecting additional sensitive data from those users, and any document capable of verifying a user's age will likely contain sensitive information. Requiring companies to collect more user data even as other states require collecting less data places businesses in the untenable position of picking which state laws to comply with, and which to unintentionally violate.[11]

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

---

[6] 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/.
[7] Engine, *More than just a number: How determining user age impacts startups* (Feb. 2024), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/65d51f0b0d4f007b71fe2ba6/1708465932202/Engine+Report+-+More+Than+Just+A+Number.pdf.
[8] *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.
[9] *See, e.g.*, Hannah Quay-de la Valle, *The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks*, Ctr. for Democracy & Tech. (May 5, 2022), https://cdt.org/insights/the-chilling-effect-of-student-monitoring-disproportionate-impacts-and-mental-health-risks/ (finding that "Monitoring programs, if not carefully implemented, can stifle growth and leave students vulnerable to the chilling effect, placing their mental health at risk").
[10] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *see also Principle (c): Data Minimisation*, U.K. Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/.
[11] 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.

coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.[12] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

Age verification and parental consent requirements for online businesses are currently being litigated in several 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 parental consent and 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 just 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 forthcoming rulings from the judiciary may be instructive in determining how, or whether, age determination requirements can be tied to granting user access to online speech. 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 taxpayers.

* * * * *

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,

Tom Mann
State Policy Manager, South
Computer & Communications Industry Association

---

[12] *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.
[13] *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).
[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.