November 13, 2025

Michigan House
Attn: House Regulatory Reform Committee
124 N Capitol Ave
Lansing, Michigan 48909

Re: HB 4388 – "Social Media Regulation Act" (Oppose)

Dear Chair Aragona and Members of the House Regulatory Reform Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 4388. 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, protecting children from harm online does not include a generalized power to restrict ideas to which one may be exposed. Lawful speech 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.

Federal courts have recently and repeatedly held that laws requiring age verification and parental consent violate the First Amendment.

Recent state legislation requiring age verification for social media sites has faced numerous constitutional challenges. Several federal courts have held that laws requiring age verification and parental consent for social media sites violate the First Amendment's guarantee of free speech. Federal courts in Ohio and Georgia have held that states cannot "prevent children from

[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).

hearing or saying anything without their parents' prior consent."[5] An Arkansas court further held that "such laws do not enforce parental authority over children's speech . . . ; they impose *governmental* authority, subject only to a parental veto."[6]

Furthermore, the bill determines whether the rules for "social media platform[s]" apply to an online service based on the service's "predominant or exclusive function." As it is difficult to objectively determine which of an online service's functions is "predominant," multiple federal courts have struck down age verification and parental consent laws using this language for being unconstitutionally vague.[7] Many online services have several functions, and the bill's multitude of carve-outs forces these services to make dozens of highly subjective judgments about whether the bill applies to them.

Numerous other federal judges have placed similar laws wholly or partially on hold until challenges can be fully reviewed, including in California,[8] Florida,[9] Texas,[10] and Utah.[11] Chief Judge Walker in the Northern District of Florida recently summarized the consensus view, stating that "like other district courts around the country, this Court simply recognizes that the First Amendment places stringent requirements on the State to avoid substantially burdening speech unless the State can show that doing so is necessary to achieve its significant interests."[12]

HB 4388's requirements undermine user privacy for users of all ages.

HB 4388 contains many requirements that undermine privacy for all users. While well-meaning, age verification mandates inherently require collecting sensitive data about users and adults. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[13] Requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a prime target for identity theft, cyberattacks, or other data breaches.[14]

Such dangers are far from hypothetical: Several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[15] Furthermore, government officials could access this sensitive data through enforcement inquiries and processes. Compounding these problems, Section 5 requires covered online services to

[5] *NetChoice v. Yost*, 778 F. Supp. 3d 923, 954 (S.D. Ohio 2025); *NetChoice v. Carr*, No. 25-cv-02422, 2025 WL 1768621 at *29 (N.D. Ga. June 26, 2025) (each quoting *Brown v. Ent. Merchs. Ass'n*, 564 U.S. 786, 795 n. 3 (2011)).
[6] *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at *31 (W.D. Ark. Mar. 31, 2025) (quoting *Brown*, 564 U.S. at 795 n. 3).
[7] *See, e.g.*, *Griffin,* 2025 WL 978607 at *34-40; *Yost*, 778 F. Supp. 3d at 957-58.
[8] *See, e.g.*, *NetChoice v. Bonta*, 770 F. Supp. 3d 1164 (N.D. Cal. 2025); *NetChoice v. Bonta*, No. 25-146 (9th Cir. Sept. 9, 2025).
[9] *See, e.g.*, *CCIA v. Uthmeier*, No. 24-cv-438, 2025 WL 1570007 (N.D. Fla. June 3, 2025).
[10] *See, e.g.*, *CCIA v. Paxton*, 747 F. Supp. 3d 1011 (W.D. Tex. 2024).
[11] *See, e.g.*, *NetChoice v. Reyes*, 748 F. Supp. 3d 1105 (D. Utah 2024).
[12] *Uthmeier*, 2025 WL 1570007 at *1.
[13] *See, e.g.*, *Fair Information Practice Principles (FIPPs)*, Fed. Privacy Council, https://www.fpc.gov/resources/fipps/; *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/.
[14] Shoshana Weissmann, *Age-Verification Legislation Discourages Data Minimization, Even When Legislators Don't Intend That*, R St. Inst. (May 24, 2023), https://www.rstreet.org/commentary/age-verification-legislation-discourages-data-minimization-even-when-legislators-dont-intend-that/.
[15] *See, e.g.*, Mark Tsagas, *Online Age Checking Is Creating a Treasure Trove of Data for Hackers*, The Conversation (Nov. 11, 2025), https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586.

retroactively verify the ages of existing users as well as prospective ones, which unnecessarily increases the risk of malicious actors accessing the data submitted.

The express parental consent requirement is also detrimental to minors. HB 4388 also requires covered "social media compan[ies]" to supply a parent or guardian who has given consent with "a password or other means for the parent or guardian to access the minor account" which would allow them to view all of the minor's posts and responses to messages. Again, while well-intentioned, this measure undermines youth privacy: Such excessive monitoring has been shown to negatively affect young people's mental health and development.[16] Furthermore, not all minors will have a parent or guardian who can provide verifiable consent (such as adopted children, children in foster care, or those whose parents have remarried).

To avoid restricting teens' access to information, HB 4388 should regulate users under 13 rather than 18 in accordance with established practices.

HB 4388 defines a minor as an individual 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.[17] 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, HB 4388 may result in denying services to all users under 18, limiting their access to needed supportive communities.

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. 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.[18]

The connected nature of social media has led some to allege that online services may be negatively impacting teenagers' mental health. However, researchers explain that this theory is

[16] *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").
[17] *See* 15 U.S.C. § 6501(1).
[18] *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/.

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,[19] individualized, reciprocal over time, and gender-specific. Indeed, as the Ohio court noted above, "nearly all of the research showing any harmful effects" for minors on social media "is based on correlation, not evidence of causation."[20]

As 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.

Currently available tools to conduct age determination are imperfect in estimating users' ages.

There is no perfect method of age determination, and the more data a method collects, the greater risk it poses to consumer privacy[21] and small business sustainability.[22] 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.[23] The report found that "smaller companies may not be able to sustain their business" if forced to implement costly age verification 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."[24]

Additionally, age verification software does not process all populations with equal accuracy. The National Institute of Standards and Technology (NIST) recently published a report evaluating six software-based age estimation and age verification tools that estimate a person's age based on the physical characteristics evident in a photo of their face.[25] The report notes that facial age estimation accuracy is strongly influenced by algorithm, sex, image quality, region-of-birth, age itself, and interactions between those factors, with false positive rates varying across demographics, generally being higher in women compared to men. CCIA encourages lawmakers to consider the current technological limitations in providing reliably accurate age estimation tools across all demographic groups.

* * * * *

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.

---

[19] 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.
[20] *Yost* at *21.
[21] 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/.
[22] 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.
[23] *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.
[24] *Id.* at 10.
[25] Kayee Hanaoka et al., *Face Analysis Technology Evaluation: Age Estimation and Verification (NIST IR 8525),* Nat'l Inst. Standards & Tech. (May 30, 2024), https://doi.org/10.6028/NIST.IR.8525.

Sincerely,

Megan Stokes
State Policy Director
Computer & Communications Industry Association