February 3, 2025

House Committee on Aging, Children and Youth, Legislative and Military Affairs
Attn: Representatives Gramlich, A. Collins, Springer
1 Capitol Mall, Fifth Floor
Little Rock, AR 72201

Re: HB 1083 – "Arkansas Kids Online Safety Act" (Oppose)

Dear Chair Barker and Members of the House Committee on Aging, Children and Youth, Legislative and Military Affairs:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 1083. 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. 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] Proposals to keep children safe online should focus on the risks and tangible harms for users in specific age ranges. While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

HB 1083 contains broad, undefined duties that will frustrate efforts to protect children online.

HB 1083 would result in contradictory standards that will not protect young internet users, and, in fact, would make them less safe. HB 1083's "duty of care" requires "covered platforms" to "take reasonable measures" to "prevent and mitigate" a broad list of defined "harm 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/.
[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).

minors" in the creation and implementation of design features. Courts have not opined on what a duty of care to protect children online means for operators of digital services. Therefore, litigation across the country will set conflicting standards to define reasonable conduct, making it impossible for businesses to operate nationwide. Clearly defined definitions and scope are crucial to ensuring that policymakers' intent is met without conflicting regulation and litigation that redefines rights and frustrates goals.

Without meaningful guidance to determine compliance through voluntary consensus standards or certification programs, for example, HB 1083 will be impossible to comply with. The net effect will be forced over-collection of data and restrictions on lawful expression, harming vulnerable communities.

HB 1083's stringent duties, safeguards, and design element mandates will force companies to collect more information, exposing vulnerable data to security risks.

Enhanced privacy protections for younger users online is a common goal. Appropriate privacy protections cannot be achieved if businesses are forced to needlessly collect more information than needed to perform a service or function of the platform. This conflicts with the principle of data minimization, which sets reasonable collection, use, or retention limitations on personal information that is processed by a digital service. This practice is especially important for children, whose data is the most sensitive.

To comply with HB 1083's duty of care, safeguards, and transparency requirements, covered platforms must employ age verification standards that require collecting additional sensitive data, including geolocation and government identification, from all users. Age verification technologies are expensive, and above all, inaccurate. They also raise concerns about false positives and negatives. Compliance also generally requires digital services to use third-party services, heightening security risks. Mandating the over-collection of children's data to intimately identify every user will not improve online safety, nor has it ever been shown to mitigate concrete harms.

HB 1083 lacks narrowly tailored definitions, creating serious compliance questions for both businesses and users.

As currently written, the bill defines a "minor" as anyone 16 or under, and a "child" as anyone 12 or under, and does not appear to use these terms clearly or consistently. Due to the myriad, almost limitless ways in which youth under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. For example, a 16-year-old conducting research for a school project can be expected to 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 "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.

Currently, many of the bill's definitions are not clear enough to enable businesses to comply. For example, "reasonable care" and "reasonable measures" are not defined in this bill. The definition of "reasonably likely to be accessed by minors" is also ambiguous, and should be more narrowly tailored to content intentionally targeted at or branded for minors when they are using the internet. Further, terms such as "addiction"—especially "addiction-like"—lack adequate scientific foundation. Absent any medical consensus on the topic, private businesses will be unable to make coherent or consistent diagnostic assessments of users. It is also very difficult to reliably describe what may constitute "harm to minors" to child users. Humans in general, especially children, have very nuanced opinions surrounding what may be harmful to them. The lived experiences of children, teens, and adults differ immensely, and businesses do not have a roadmap to users' lived experiences, and what could potentially cause them harm.

Legislation should clearly define the applicability standards set within. Without clear standards in place, digital services providers will not know how to comply or will be forced to expend considerable resources that impose barriers to competition and innovation.

HB 1083's definition of "covered platform" broadly encompasses most websites and online applications that a minor is "reasonably likely" to use. In many instances, HB 1083 does not require actual knowledge that a minor uses the platform. Given this broad application, covered platforms will be required to utilize data collection intensive practices like age and identity verification standards to avoid facing liability.

Finally, HB 1083 imposes a contradictory knowledge standard for new duties which suggests actual subjective knowledge, but will instead be interpreted as reasonable objective knowledge, a substantially broader legal standard. To avoid liability, privacy-enhancing services like end-to-end encryption or other protective measures will be greatly restricted.

If enacted, HB 1083 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 vague duty of care and lack of narrowly tailored definitions 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.[5] 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. An online central meeting place where kids can share their experiences and find support can have positive impacts.

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

[5] *See, e.g.*, *Reno v. ACLU*, 521 U.S. 844, 874-75 (1997).

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,[6] individualized, reciprocal over time, and gender-specific. A study conducted by researchers from several leading universities found that there is no evidence that associations between adolescents' digital technology engagement and mental health problems have increased.[7] Particularly, the study shows that depression has virtually no causal relation to TV or social media.

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.

HB 1083's ambiguous duties will mandate restrictive content and design practices that silence voices.

For more than 200 years, courts have upheld protections enshrined in the First Amendment which protect individuals and businesses from government interference that blocks or compels speech.[8] These protections are crucial for internet companies to engage in appropriate content moderation practices that limit dangerous and unwanted content online. HB 1083 implements restrictions on design features that will lead to increased data collection from minors and over-removal of constitutionally protected content.

The internet is an integral component of community building and social expression. In light of the extraordinary volume of internet communications, imposing liability rules that mandate increased review and removal of constitutionally protected speech is a chilling barrier that only hurts internet users. Communities who may be unable to freely express or find like-minded individuals offline will be further cut off from these valuable resources online.

Arkansas should not impede continuing efforts by private businesses to moderate content on their services, including through the use of algorithms.

Just as digital services do not serve all users, they do not publish all content. In addition to prohibiting illegal content as required by relevant state and federal laws, many digital services remove content that is dangerous, though not inherently illegal. This includes, for example, content that exhorts users to self-harm or encourages young people to engage in dangerous or destructive behavior.

Setting aside the matter of whether the government should impose upon private companies the obligation to host or take down lawful speech, which raises First Amendment concerns, digital services are already taking aggressive steps to moderate and remove dangerous and

[6] 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.
[7] Amy Orben, *et al.*, *There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased*, Sage Journals (May 3, 2021), https://journals.sagepub.com/doi/10.1177/2167702621994549.
[8] *See, e.g.*, *W. Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624 (1943); *Erznoznik*; *Reno*.

illegal content consistent with their terms of service.[9] Services deliver on the commitments made to their user communities with a mix of automated tools and human review.

Recent state legislation on child safety 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.[10] 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 the judiciary to more fully examine this issue before burdening businesses with legislation that risks being invalidated and passing on expensive litigation costs to taxpayers.

* * * * *

While we share the concerns of the sponsors and the House Committee on Aging, Children and Youth, Legislative and Military Affairs 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,

Megan Stokes
State Policy Director
Computer & Communications Industry Association

[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.*, *NetChoice v. Bonta*, 113 F.4th 1101(9th Cir. 2024); *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).