



February 21, 2025

House Committee on Consumer Protection and Business  
John L. O'Brien Building  
P.O. Box 40600  
Olympia, WA 98504-0600

## Re: HB 1834 – "Relating to protecting Washington children online" (Oppose)

Dear Chair Walen, Ranking Member McClintock, and Members of the House Consumer Protection & Business Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 1834. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.<sup>1</sup> 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.<sup>2</sup> 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.<sup>3</sup>

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.<sup>4</sup> While CCIA shares the goal of increasing online safety, this bill presents the following concerns.

### Requirements under HB 1834 are not administrable or well defined, creating serious compliance questions for both businesses and users.

The bill's definitions section begins with the phrase "unless the context clearly requires otherwise," followed by definitions of the key terms. If the bill's definitions can be altered based on a concept as vague as "context," a covered social media platform cannot know in

<sup>1</sup> 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>.

<sup>2</sup> Competitive Enterprise Institute, *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/>.

<sup>3</sup> 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/>.

<sup>4</sup> *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).

advance whether it is complying with the law or not. Such a provision is too vague to meet the Fourteenth Amendment’s Due Process Clause requirements.

Additionally, many of the specific requirements for covered businesses are too vague for businesses to know whether they are complying with the law. For instance, Section 2(1) applies to products and services that are “reasonably likely to be accessed by minors” without any indication as to how covered businesses can objectively assess such likelihood. Such businesses must “estimate the age of minor users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business” or apply the data protections they afford to minors to all users. A covered business has no way of knowing what law enforcement would consider “a reasonable level of certainty appropriate to the risks” of their practices. Similarly, Section 2(2) requires covered businesses to implement age assurance measures that are “proportionate to the risks and data practice of an online service, product, or feature.” These are highly subjective requirements that cannot be enforced in a non-arbitrary manner.

### **Terms such as “addictive” in this online context lack adequate scientific foundation.**

Humans engage in various compulsive and repetitive behaviors — some of which may negatively impact physical and/or mental health. Compulsive behaviors could range from binge eating unhealthy foods to exercising excessively to watching favorite shows for hours on end. However, certain regular activities do not necessarily amount to “addictions”. The most recent edition of the *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision (DSM-5-TR)* declined to include definitions for “Internet gaming disorder,” “Internet addiction,” “excessive use of the Internet,” or “excessive use of social media,” noting that “[g]ambling disorder is currently the only non-substance-related disorder included in the *DSM-5-TR* chapter ‘Substance-Related and Addictive Disorders.’”<sup>5</sup>

The relationship between social media use and youth mental health also lacks conclusive evidence. When the U.S. Surgeon General released an Advisory entitled *Social Media and Youth Mental Health*, many were quick to highlight only the harms and risks it detailed. However, the Advisory is much more nuanced and also discusses many potential benefits of social media use among children and adolescents. For example, the Advisory concludes that social media provides young people with communities and connections with others who share identities, abilities, and interests.<sup>6</sup> It can also provide access to important information and create spaces for self-expression. Research further details that social media can especially benefit marginalized youth, including racial, ethnic, sexual, and gender minorities, as online peer support can mitigate the stresses they face.<sup>7</sup>

Without any medical consensus on the topic, private businesses cannot be expected to make coherent or consistent diagnostic assessments of what might constitute an “addictive feed” or

<sup>5</sup> Am. Psychiatric Ass’n, *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision* (2022).

<sup>6</sup> Off. of the Surgeon Gen., U.S. Department of Health & Human Services, *Social Media and Youth Mental Health: The U.S. Surgeon General’s Advisory, Social Media Has Both Positive and Negative Impacts on Children and Adolescents* (2023), <https://www.ncbi.nlm.nih.gov/books/NBK594763/>.

<sup>7</sup> *Id.*; see also Jennifer Marino et al., *Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, *J. Med. Internet Rsch.* (Sept. 22, 2021), <https://www.jmir.org/2022/9/e38449>.

“addictive internet-based service or application.” Compounding these problems, the definitions in HB 1834 of “addictive feed” and “addictive internet-based service or application” are not even based on any criteria tangentially related to “addiction.” Rather, the bill posits that a feed whose content is generated “based, in whole or in part, on information provided by the user, or otherwise associated with the user or the user’s device” is an allegedly “addictive feed.” Such a definition is highly counterintuitive: a simpler and clearer approach would be to specify what types of data businesses may process under what circumstances, rather than attempting to relate such rules to vague concepts like “addiction.”

### **If enacted, HB 1834 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.<sup>8</sup> 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.<sup>9</sup>

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 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,<sup>10</sup> 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.<sup>11</sup> 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.

<sup>8</sup> See, e.g., *Reno v. ACLU*, 521 U.S. 844, 874-75 (1997).

<sup>9</sup> *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/>.

<sup>10</sup> 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>.

<sup>11</sup> 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>.

## 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<sup>12</sup> and small business sustainability.<sup>13</sup> 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.<sup>14</sup> 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.”<sup>15</sup>

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.<sup>16</sup> 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.

## Age verification 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.<sup>17</sup> After 25 years, age authentication still remains a vexing technical and social challenge.<sup>18</sup>

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.<sup>19</sup> CCIA anticipates that these forthcoming

<sup>12</sup> 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/>.

<sup>13</sup> 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>.

<sup>14</sup> *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](https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf).

<sup>15</sup> *Id.* at 10.

<sup>16</sup> 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>.

<sup>17</sup> *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).

<sup>18</sup> 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>.

<sup>19</sup> 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.



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 Washington 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,

Aodhan Downey  
State Policy Manager, West  
Computer & Communications Industry Association

---

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).