



March 7, 2025

Office of Governor Gordon  
The Honorable Mark Gordon  
Wyoming State Capitol  
200 W 24th St.  
Cheyenne, WY 82002

## Re: HB 43 – "Age verification for websites with harmful material" (Veto Request)

Dear Governor Gordon:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully request a veto of HB 43. 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. Lawful speech 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.

---

<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/> (last updated Feb. 19, 2025).

<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).



## Requirements under HB 43 are not administrable or well defined, creating serious compliance questions for both businesses and users, and a chilling effect on free speech.

HB 43 would create many vaguely defined obligations for businesses, leaving them unable to know whether they are violating the law. The bill's definitions broadly reference a range of types of businesses, from "access software providers" to "covered platforms" to "interactive computer services." It would require that "any covered platform shall perform reasonable age verification methods to verify the age of all persons accessing or attempting to access the material and shall prevent access by minors to the material." The "reasonable age verification methods" oddly include credit or debit cards, which may pose fraud or security risks, as well as "any other means or method that reliably and accurately can determine whether a user of a covered platform is a minor," with neither "reliably" nor "accurately" defined or appearing elsewhere in the bill's text.

Conflating "harmful to minors" and "obscene" with "the bill's intended target of pornography" would sweep in a broad range of First Amendment-protected speech, as ACLU Wyoming notes.<sup>5</sup> Further, HB 43 creates significant liability concerns due to the subjective nature of what may be considered "harmful to minors" or "obscene." 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 Wyoming law appears to acknowledge.<sup>6</sup> Covered platforms cannot be expected to make such subjective assessments, and will inevitably engage in over-filtering to ensure compliance. Requiring businesses to make such subjective assessments is especially risky given the bill's private right of action, as further detailed below.

## To avoid restricting teens' access to information, HB 43 should regulate users under 13 rather than 18 in accordance with established practices.

HB 43 defines a minor 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 "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.

<sup>5</sup> ACLU of Wyoming, House Bill 43, <https://www.aclu-wy.org/en/legislation/house-bill-43> (last accessed Feb. 25, 2025).

<sup>6</sup> HB 43 § 14-3-501(a)(viii) points to Wyo. Stat. § 6-4-301(a)(iii) for the definition of "obscene," which appears to codify *Miller v. California*, 413 U.S. 15, 24 (1973).



## **If enacted, HB 43 may result in denying services to all users under 18. Limiting access to the internet for children curtails their ability to access information and supportive communities that may not be available 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. 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>7</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>8</sup> individualized, reciprocal over time, and gender-specific.

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<sup>9</sup> and small business sustainability.<sup>10</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>11</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>12</sup>

<sup>7</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>8</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>9</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>10</sup> Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Feb. 2024), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+T+han+Just+A+Number+-+Updated+August+2024.pdf>.

<sup>11</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>12</sup> *Id.* at 10.

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>13</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>14</sup> After 25 years, age authentication still remains a vexing technical and social challenge.<sup>15</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>16</sup> 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 Wyoming taxpayers.

## **Investing sole enforcement authority with the state attorney general would be beneficial to consumers and businesses alike.**

By creating a new private right of action, this measure allows plaintiffs to advance frivolous claims with little evidence of actual injury. Such lawsuits also prove extremely costly and time-intensive, with the costs being passed on to individual Wyoming consumers. Such a measure would disproportionately impact smaller businesses and startups across the state. Further, investing sole enforcement authority with the state attorney general allows for the leveraging of technical expertise concerning enforcement authority, and allows public interest to determine which enforcement actions are brought.

<sup>13</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>14</sup> *Reno v. ACLU*, 521 U.S. 844, 855-57, 862 (1997).

<sup>15</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>16</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. 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).



\* \* \* \* \*

While we share the concerns of Rep. Martha Lawley and other cosponsors regarding the safety of young people online, we encourage Governor Gordon to resist signing legislation that is not adequately tailored to this objective and respectfully request a veto of HB 43.

Sincerely,

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