



April 1, 2026

House Committee on Judiciary
Alaska State Capitol
120 4th St
Juneau, AK 99801

Re: HB 318 - “An Act relating to use of social media platforms by minors” (Oppose)

Dear Chair Gray, Vice Chair Kopp, and Members of the House Committee on Judiciary:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 318. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.¹ Proposed regulations on the intrastate provision of digital services therefore can have a significant, nationwide impact on CCIA members.

CCIA firmly believes that children are entitled to security and privacy online. Our members have designed and developed 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 However, while CCIA shares the goal of increasing online safety for minors, HB 318 introduces significant constitutional, operational, and privacy concerns that would negatively impact Alaska residents and businesses.

The bill’s required disclosures violate the First Amendment.

HB 318 requires covered businesses to “submit an annual report to the attorney general that includes”, among other things, “a description of any internal assessments conducted regarding engagement or wellbeing of minors. The U.S. Court of Appeals for the Ninth Circuit has ruled multiple times that such mandatory disclosures constitute compelled speech in violation of the First Amendment.³ In 2024, the court held that “requir[ing] the forced creation and disclosure of highly subjective opinions about content-related harms” constitutes “State attempts to indirectly censor the material available... online[] by delegating the controversial question... to the companies themselves.”⁴ Such requirements therefore “fall[] well short of satisfying strict First Amendment scrutiny” and are unconstitutional.⁵

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 Inst., *Children Online Safety Tools*, <https://cei.org/children-online-safety-tools/> (last updated June 10, 2025).

³ See, e.g., *NetChoice v. Bonta*, 113 F.4th 1101 (9th Cir. 2024); *X Corp. v. Bonta*, 116 F.4th 888 (9th Cir. 2024).

⁴ *NetChoice*, 113 F.4th at 1122.

⁵ *Id.*

The bill's requirements undermine user privacy for users of all ages.

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.⁶ Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.⁷ Furthermore, government officials could access this sensitive data through enforcement inquiries and processes.

While well-meaning, the bill's requirements will inevitably lead to the collection of sensitive data about users and adults. Such policies run contrary to the data minimization principles underlying federal and international best practices for privacy protection.⁸ Furthermore, the more data a service is forced to collect, the greater risk it poses to consumer privacy and small business sustainability.⁹ A recent Digital Trust & Safety Partnership (DTSP) report, *Age Assurance: Guiding Principles and Best Practices*, 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.”¹⁰

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 coverage of the population; and 3) respecting the protection of individuals' data, privacy, and security.¹¹ Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people. As Senator Lenney noted recently, “We’re building a surveillance apparatus for kids. We’re mandating social media companies digitally surveil our kids.”

⁶ 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/>.

⁷ 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>.

⁸ 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/>.

⁹ Engine, *More Than Just a Number: How Determining User Age Impacts Startups* (Aug. 2024),

<https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/66ad1ff867b7114cc6f16b00/1722621944736/More+Than+Just+A+Number+-+Updated+August+2024.pdf>.

¹⁰ *Age Assurance: Guiding Principles and Best Practices*, Digital Trust & Safety Partnership (Sept. 2023) at 10,

https://dtspartnership.org/wp-content/uploads/2023/09/DTSP_Age-Assurance-Best-Practices.pdf.

¹¹ *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>.

Terms such as “addiction” or “addictive” in an online context lack an adequate scientific foundation.

The bill’s broad definition of “addictive design features” uses the term “addiction” outside its defined scientific context. 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.’”¹²

The connected nature of social media has led to allegations that online services are negatively impacting teenager’s mental health. However, researchers argue that this theory is not well supported by existing evidence and often mirrors the “moral panic” associated with new technologies. Much research on social media and adolescent health (including the National Academies of Sciences, the University of Oxford, the American Psychological Association, and the Journal of Pediatrics) has found that social media does not cause changes in adolescent health at the population level.¹³ Even the Surgeon General’s Social Media and Youth Mental Health advisory acknowledges the benefits of social media, including social connection, information sharing, and civic engagement.¹⁴ Indeed, as a federal court recently noted, “nearly all of the research showing any harmful effects” for minors on social media “is based on correlation, not evidence of causation.”¹⁵

The bill incentivizes overcollection of minors’ data.

HB 318 also requires that covered businesses not send minors notifications “between the hours of 10:00 p.m. and 7:00 a.m.” Such requirements inevitably require that covered operators track when it is nighttime in a given device’s location. This requirement therefore effectively mandates location-based tracking of minors’ devices, thus undermining the privacy of the very population the bill is designed to protect. Requiring covered operators to track their users serves no benefit, particularly since covered operators regularly offer users the option to turn off notifications themselves.

¹² Am. Psychiatric Ass’n, *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision* (2022).

¹³ Regina Park, *The Internet Isn’t Harmful to Your Mental Health, Oxford Study Finds*, Disruptive Competition Project (Jan. 29, 2024),

<https://project-disco.org/innovation/the-internet-isnt-harmful-to-your-mental-health-oxford-study-finds/>.

¹⁴ Mike Masnick, *Warning: Believing The Surgeon General’s Social Media Warning May Be Hazardous To Teens’ Health*, Techdirt (June 18, 2024),

<https://www.techdirt.com/2024/06/18/warning-believing-the-surgeon-generals-social-media-warning-may-be-hazardous-to-teens-health/>.

¹⁵ *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).



The bill’s requirements are not well-defined.

HB 318 determines a covered service’s responsibilities in part based on whether “the controller knows or reasonably should know that the consumer is a minor”. It is, however, difficult to objectively determine when a controller “should know” that a user is a minor if the controller does not have actual knowledge. Consequently, these standards risk being applied arbitrarily and inconsistently. Framing online services’ obligations in such vague terms leaves them unable to know whether they are violating the law, or what corrective measures they must take.

Furthermore, the bill does not create a set list of design features that covered services must not provide to minors. Rather, after listing several features, the bill bans “any other feature that the attorney general determines by regulation encourages prolonged or compulsive use of a social media platform.” The bill does not specify what constitutes “compulsive use” or when a given design feature “encourages” such use. Moreover, any improvement in a website’s quality or functionality could be said to “prolong[]” use of the website. Consequently, covered entities will have no way of knowing what measures they need to institute, or how they are to know whether they are succeeding. Defining covered services’ obligations using such vague and subjective terms risks arbitrary and inconsistent application of the law.

To avoid restricting teens’ access to information, HB 318 should regulate users under 13 rather than 18 in accordance with established practices.

HB 318’s regulations apply to individuals less than 18. Due to the nuanced ways in which children and teens 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 encounter, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. We would suggest regulating users based on whether they are under 13 to align with the federal Children’s Online Privacy Protection Act (COPPA) standard.¹⁶ 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.

* * * * *

We appreciate your consideration of CCIA’s comments and stand ready to provide additional information as you consider proposals related to technology policy.

Sincerely,

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

¹⁶ See 15 U.S.C. § 6501(1) (1998).