TAXPAYERS PROTECTION ALLIANCE

April 2, 2026

House Judiciary Committee
Alaska State Legislature
1500 W Benson Blvd
Anchorage, AK 99503

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

On behalf of the millions of taxpayers and consumers we represent, the Taxpayers Protection Alliance (TPA) urges you to reconsider House Bill (HB) 318, a bill to regulate social media platforms. While the goal of protecting children online is a noble one, this bill falls short in numerous ways.

HB 318's conception of "addiction" is overly broad. The bill defines "addictive design feature" to include 1) "content that loads continuously or as the user scrolls down the page…," 2) "pages with no visible or apparent end or page breaks," or 3) a "video that begins to play automatically…" (as well as other features to be designated by the Attorney General). This definition does not describe anything approaching the common usage of "addiction"; it merely describes the basic and heretofore unobjected-to features of the internet. It is worthwhile to consider what this three-pronged definition might encompass. To take but one example, the first and second prongs could bar a video service like YouTube's search feature from providing a high-school student extensive resources for his or her class presentation. Further, under this definition, a teenager reading news articles on a local newspaper's website or scrolling through posts on a community forum would be consuming content delivered via "addictive design features." The bill makes no distinction between a platform engineered to maximize compulsive engagement and useful digital tools that pose little harm to anyone.

Moreover, the bill delegates to the Attorney General unlimited authority to designate "additional addictive design features" by regulation. This open-ended grant of authority provides no meaningful limiting principle and invites arbitrary enforcement.

The definition "known minors" encompasses users the platforms "knows or *reasonably should know*" (emphasis added) are underage. This vague language creates a legal trap.

Platforms that do not verify user ages can claim ignorance—but the "reasonably should know" standard exposes them to liability whenever circumstantial evidence suggests a user may be a minor. A username referencing a high school, profile content mentioning homework, or activity patterns consistent with a school schedule could all establish constructive knowledge.

Faced with this exposure to liability, rational platforms will likely implement age verification not because the bill explicitly requires it, but because it is the only reliable way to establish that a user is not a "known minor" per the bill's text.

Age verification requires users to submit a tremendous amount of sensitive personal information, which then becomes stored in large databases, liable to be hacked or to fall victim to data breaches. This information usually takes the form of scans of government-issued identification documents or biometric data, such as facial scans. It would directly contradict the goal of ensuring children's safety in the digital world for the State to mandate that children serve up their data to technology platforms, exposing that data to bad actors.

Children already face vast privacy dangers. As noted by the R Street Institute last year, "The problem is so extensive that research by Experian suggests that 25 percent of children will be victims of identity fraud or theft

by the time they are 18."[1] Moreover, R Street continues, "More than half of minors who were victims of identity theft report being denied access to credit at least once because of it, and some deal with the consequences for a decade or more. Some have even acquired a lifelong criminal record for an offense committed by the thief that stole their identity." Requiring children to provide sensitive personal information to access everyday digital tools—which are becoming ever more ubiquitous—would only compound these dangers.

Recent experience demonstrates the dangers of mandating the storage of large amounts of sensitive information in vulnerable databases—even those purported to be secure. In the digital age, hacks and data leaks are commonplace. Indeed, a Duke University analysis found that more than four in five of companies say they have dealt with a hack.[2] Tech companies—including some of the largest and best protected companies—routinely fall prey.[3]

Even third-party age verifiers, which specialize in the business of age verification, experience cyber incidents. "[T]hese services have suffered cyber events, too," as TPA noted in its amicus brief filed at the Supreme Court in *NetChoice v. Fitch*. "Outabox, which provided facial-recognition services to various in-person businesses, announced a massive cybersecurity breach in 2024 resulting in the piracy of more than one million consumer records. AU10TIX, an identity-verification service used by recognizable platforms like Uber, TikTok, X, and LinkedIn, is another victim of cybercrime."[4]

Even the most supposedly privacy-protective age-verification mandates, such as those recently enacted in France, have undermined safety and privacy.[5] Supreme Court Justice Alito may have put it best during the oral arguments in *Free Speech Coalition v. Paxton*: "There have been hacks of everything."[6]

HB 318 misses the mark in several ways that will ultimately harm Alaskans. For these reasons, TPA urges you to reconsider this legislation.

Sincerely,

David Williams
President

[1] https://www.rstreet.org/commentary/child-identity-theft-is-a-huge-problem-the-solutions-are-simple/
[2] https://cfosurvey.fuqua.duke.edu/press-release/more-than-80-percent-of-firms-say-they-have-been-hacked/
[3] https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html
[4] https://www.protectingtaxpayers.org/press/watchdog-group-files-amicus-brief-defending-mississippian-social-media-users/
[5] https://aiforensics.org/uploads/AIF_report_AgeGO_porn_platforms.pdf
[6] https://www.supremecourt.gov/oral_arguments/argument_transcripts/2024/23-1122_7m58.pdf