From: Raina Collins
To: Senate Community and Regional Affairs; Rep. Ky Holland; Sen. Scott Kawasaki
Subject: HB47
Date: Wednesday, March 25, 2026 2:04:38 PM

I am a resident and a registered voter. I've lived in Alaska my entire life. I am a cybersecurity professional with 10+ years of experience. I have an Associates, Bachelors, and Masters degree in cybersecurity. I am asking you to review my rebuttal. (Written by AI, validated by a human)

Rebuttal to HB47 § 45.50.650 — Age Verification and Parental Consent

---

This Won't Actually Keep Kids Off Social Media

Other states and countries have tried nearly identical laws, and kids simply work around them. When Florida's age verification law took effect on January 1, 2025, a surge of 1,150% in VPN demand was detected almost immediately — because VPNs let users make it appear they are somewhere the law does not apply. The Electronic Frontier Foundation confirmed the pattern is not unique to Florida: when platforms block access or require invasive verification, it drives people to sites that operate outside the law — platforms that often pose greater safety risks. Kids do not stop using social media — they just move somewhere less regulated and less safe - as confirmed by Pinterest. Minors realized Pinterest was not monitored as much as Snapchat and TikTok and thus they were using the messaging feature inside the platform.

Courts have confirmed this practical reality. The judge who permanently blocked Arkansas's nearly identical law in March 2025 wrote that "there is no evidence that the Act will be effective in achieving the State's goal of protecting minors."

It Forces Every Adult to Hand ID to a Private Company

Section (b) requires platforms to verify the age of every user — not just suspected minors. That means every adult Alaskan must prove to a corporation that they are not a child just to use social media. This creates a brand new privacy exposure that didn't exist before.

To verify an adult's age, platforms collect government IDs or biometric data. That data gets stored, shared with vendors, and becomes a target. This already happened: Pornhub's parent company stated that requiring hundreds of thousands of sites to collect significant amounts of highly sensitive personal information is putting user safety in jeopardy.The EFF has also documented that age verification requirements subject every user to surveillance as a condition of participation — a significant burden for a law that demonstrably does not work.

Labeling a Child's Account Creates Its Own Privacy Risk

The parental consent framework requires platforms to affirmatively flag certain accounts as

belonging to verified minors. That creates a labeled dataset of children tied to their behavior, device, and location data — with no security requirements attached. **HB47 says nothing about how that data must be stored, secured, or prevented from being sold or breached.**

This Type of Law Gets Struck Down

Alaska would not be the first state to try this, and it would not be the first to lose in court. Arkansas's law — which required the same age verification and parental consent structure — was permanently blocked by a federal judge who found it violated both the First and Fourteenth Amendments. The court found the law "erects barriers to accessing entire social media platforms rather than placing those barriers around the content or functions that raise concern." State efforts to limit minors' access to social media with an age verification gate are likely to find the First Amendment a persistent obstacle. Alaska would be spending public funds on a legal fight it is very likely to lose, without protecting a single child in the meantime.

A Better Path Exists

The EFF recommends better default protections for parents and young people that do not invade their privacy, combined with education and media literacy to prepare both minors and adults for the dangers of digital life. Platform design obligations — requiring safer defaults, limiting algorithmic targeting of minors, and restricting data collection — can meaningfully protect kids without forcing every adult in the state to submit identity documents to Facebook.

Please do not enact this section of HB47. It is more catastrophic than the sponsors may have understood.

Sincerely,
Raina Collins
[redacted]

1. Florida VPN Surge vpnMentor Research Team. "VPN Demand Surge in Florida after Adult Sites Age Restriction Kicks In." vpnMentor, January 2, 2025. https://www.vpnmentor.com/news/vpn-demand-surge-florida/

2. EFF — Age Verification Drives Users to Less Safe Platforms Electronic Frontier Foundation. "The Year States Chose Surveillance Over Safety: 2025 in Review." EFF Deeplinks, January 9, 2026. https://www.eff.org/deeplinks/2025/12/year-states-chose-surveillance-over-safety-2025-review

3. Pornhub/Aylo Statement on Privacy Risk of ID Collection Electronic Frontier Foundation. "VPNs Are Not a Solution to Age Verification Laws." EFF Deeplinks, January 2025. https://www.eff.org/deeplinks/2025/01/vpns-are-not-solution-age-verification-laws

4. EFF — Every User Subjected to Surveillance as Condition of Participation Electronic Frontier Foundation. "The Year States Chose Surveillance Over Safety: 2025 in Review." EFF

Deeplinks, January 9, 2026. https://www.eff.org/deeplinks/2025/12/year-states-chose-surveillance-over-safety-2025-review

5. Discord Data Breach — 70,000 Government ID Photos Exposed Salon. "Social Media Age Verification Is Full of Risks and Unclear Rewards." Salon.com, February 12, 2026. https://www.salon.com/2026/02/11/social-media-age-verification-is-full-of-risks-and-unclear-rewards/

6. EFF — Age Verification Barriers Along Lines of Race, Disability, Gender Identity, Immigration Status Electronic Frontier Foundation. "Who's Harmed by Age Verification Mandates?" EFF.org, December 2025. https://www.eff.org/pages/whos-harmed-age-verification-mandates

7. EFF — LGBTQ+ Youth, Foster Youth, and Parental Consent Harms Electronic Frontier Foundation. "10 (Not So) Hidden Dangers of Age Verification." EFF Deeplinks, December 12, 2025. https://www.eff.org/deeplinks/2025/12/10-not-so-hidden-dangers-age-verification

8. Arkansas Law Permanently Blocked — No Evidence of Effectiveness NetChoice. "NetChoice Secures Key Victory for Free Speech: Court Permanently Blocks Arkansas Age Verification Law." NetChoice.org, April 8, 2025. https://netchoice.org/netchoice-secures-key-victory-for-free-speech-court-permanently-blocks-arkansas-age-verification-law/

9. Arkansas Court Opinion — First and Fourteenth Amendment Violations Arkansas Advocate. "Federal Judge Declares Arkansas Social Media Age-Verification Law Unconstitutional." April 1, 2025. https://arkansasadvocate.com/2025/04/01/federal-judge-declares-arkansas-social-media-age-verification-law-unconstitutional/

10. First Amendment as a Persistent Obstacle to Age Verification Laws Bloomberg Law. "Arkansas Social Media Age-Check Law's Demise Threatens Others." April 4, 2025. https://news.bloomberglaw.com/litigation/arkansas-social-media-age-check-laws-demise-threatens-others

11. EFF — Better Default Protections and Media Literacy as Alternatives Electronic Frontier Foundation. "The Year States Chose Surveillance Over Safety: 2025 in Review." EFF Deeplinks, January 9, 2026. https://www.eff.org/deeplinks/2025/12/year-states-chose-surveillance-over-safety-2025-review

From: seward@tuta.com
To: Senate Community and Regional Affairs
Subject: HB47
Date: Tuesday, March 24, 2026 6:52:56 PM

Dear Members of the Senate Community and Regional Affairs Committee,

I am a Seward resident writing to oppose the social media provisions in HB 47, specifically the age verification mandate in AS 45.50.650.

The bill requires every Alaskan to verify their age on any platform that hosts user-generated content. The definition of "social media platform" is broad enough to cover nearly any website with comments, forums, or uploads. The bill does not specify how verification must be done, leaving the door open for methods that collect sensitive personal data with no privacy protections written into the law.

Parental controls already exist at the device, browser, router, and carrier level. Those tools put control in the hands of parents without forcing every adult in the state through an identity check to use the internet.

I support the portions of HB 47 that address AI-generated CSAM and deepfakes. Those provisions target real harms. The social media sections do not. They create compliance burdens that major platforms may absorb but smaller sites will not, and they push minors toward unregulated platforms that will never comply with Alaska law.

Please remove or substantially rework Sections 24 and 30 before advancing this bill.

Thank you for your time.

From: [redacted]
To: Senate Community and Regional Affairs
Subject: Concerned about HB 47
Date: Friday, March 20, 2026 5:51:24 PM

My name is James, and I'm a constituent in Anchorage. I was advised by a senate staffer to email this address. I saw in the ADN that HB 47 had passed the house a while ago, and I don't think social media age verification is a good idea. The primary function of these laws is to get people's identity stolen. Age verification does not successfully protect children; its track record on that so far has been miserable. Just look at Roblox: it has age verification, but is a hellhole of child abuse and exploitation regardless. Leaving that provision in would primarily punish adults for using the internet at all, while doing nothing to protect our kids. This would also provide precedent/capability for people to end up on government lists for visiting certain websites deemed politically inconvenient.

I'm all for criminalizing AI for generating nudes, regardless of who the nudes are of, so that much is a good idea, but the age verification provisions are flawed as a concept, not fixable, and they need to go.

Thank you for your time,
James

From:	Kolten Janes
To:	Senate Community and Regional Affairs
Subject:	HB 47 would have the opposite of it"s intended effect
Date:	Tuesday, March 24, 2026 6:48:40 PM

The short summary is the current bill would filter kids into using illegal websites that do not care about the laws in other countries. Compliant and safe websites will block the child from accessing their website and the child will just move on to the dangerous none-compliant websites. These websites are filled with malware, viruses, and attempts to steal your data. Here are some other issues I have with the bill:

Firstly, the method they use to verify age is not secure. As recent as October a third-party service used by discord to verify ages was breached and over 70,000 government issued IDs and IP addresses were stolen.

Secondly, biometric data is a powerful tool used to steal identities. Lawmakers are casually requiring us to give up this data without understanding the serious security risks involved.

Thirdly, we already have content filtering tools on the local network that are far more reliable. You can restrict websites using your router, the computer your child uses, their phone, or through your wireless carrier. Parental controls already exist.

From:	Jack Butto
To:	Senate Community and Regional Affairs
Subject:	Major Concerns over House Bill 47
Date:	Sunday, March 15, 2026 2:30:05 PM

Hello! My name is Jack. I lived in Anchorage, Alaska, since I was born and I'm writing this email due to concerns I have over Alaskan House Bill 47 regarding the protection of minors on the internet. I read over the bill and while I do agree with a lot of its contents, I have a very major concern regarding the portion regarding people having to verify their age for social media if this bill passes. I fear that if people are required to give any sort of information regarding their identification online, it only will end up enabling vulnerabilities for not only minors but for adults as well. Specifically from hackers with malicious intent to steal people's identities, data, and other personal effects.

We all live in a day and age where a majority of the world uses the internet for just about anything online, not just kids. Many people's livelihoods revolve around the internet, be it for leisure activities or, as becoming more and more common in the past decade alone, their jobs. And disclosing any sort of information regarding people's identities, especially on social media, which is routinely targeted by hackers, I fear this will only be the start of a growing crisis for people of all ages. Not only would hurt the sanctity of privacy, especially in an increasing societal culture revolving around the internet, but opens ways of attacks for malicious predators regardless of age. From people who would steal identities to buy property in other people's name to hackers who charge outrageous sums of money on stolen data they hacked from victims on the internet.

When I was a kid, we were taught in school never to give any information about ourselves to strangers online. Be it to people we don't know to people we do, as we never know who may be watching online and waiting to steal what we consider private. This is very true to this day, if not more so, be it for children or adults. We should continue to be anonymous to protect ourselves from people with malicious intent, not allow ourselves to enable hackers to take advantage of us. I know some will say that there are safeguards in place for this kind of fear, but with how frequent data breaches happen all over the world, like with X (formerly known as Twitter), I have zero faith in such promises. There is no guarantee in the world that can convince me that I, or anyone, be they a child or an adult, will be safe from hackers online if I have to give something valuable, like my age or identity. It is also why I'm very careful writing this email here because I fear that hackers or bad actors will try get personal details even when I'm trying to address public issues like this bill.

With all that said, I ask that age verification be removed from this bill. Don't get me wrong, I agree with mostly everything else on the bill regarding child safety, but I can't in good faith trust age verification to protect me or any child from online predators. Again, my greatest fear that this will only allow malicious and vile people to find ways to use this verification system as a way to bring only harm to everyone who uses it. It's not a matter of if will happen, but *when*.

That's why we Alaskans have to be better than this. *Should* better than this. We shouldn't allow anyone, be they relatives or the government, to regulate social media with things that could easily harm us regardless of the intent. And the intent is admirable, but the execution and method is something I can't get behind. So please, don't include Age Verification in Bill 47! I don't want to fear for my livelihood, or that of my family's, every time I use social media. And I hope that my fellow Alaskans feel the same fear that I do and oppose this very real risk to our privacy and our data.

Thank you for your time, and I hope you all have a wonderful day.

Testimony in Opposition to HB47, Article 5A

Dear Members of the Committee:

I am writing to respectfully voice my opposition to HB47, Article 5A. The problem of young people having bad social-media habits is not the same as the problem of CSAM, and they should not be wedged together into the same bill in order to make a bad solution to one part of addressing the other. And make no mistake: Article 5A, the portion directed to social media, is not a good bill.

I. OVERBROAD SCOPE

Start with the bill's definition of "social media platform":

> an online service, application, or Internet website that allows users to create, share, or view user-generated content, including text, images, videos, or audio[.]

This encompasses virtually any website that makes user-generated content available at all. This includes not just those few mega-corporations that everyone justifiably dislikes, but also the following:

- Discussion forums for niche interests (crochet, identifying local plants, discussing a favorite obscure TV show, etc.), that are run by volunteers, take no measures to monopolize attention or prolong the time users spend there, run minimal to no advertising, and could not by any stretch of the imagination be considered harmful to teenagers.
- The websites of many state legislatures, which show written testimony created by citizens who open accounts to comment upon bills.
- The websites of local newspapers and TV stations, which offer comment sections attached to their news stories.
- Scirate, a nonprofit website where scientists and mathematicians bookmark and comment upon technical publications that have yet to be formally peer reviewed.
- Archive Of Our Own (AO3), a nonprofit website that hosts fanfiction and provides users with the ability to comment upon, bookmark and send kudos to the works of other users.
- Codeberg, a platform for sharing and collaborating upon open-source software.
- Stack Exchange, a network of user-driven Q&A websites on many topics that began with computer programming and has since expanded to include subjects across the sciences and the arts.
- LibriVox, a platform where volunteers create and share audiobooks made from works in the public domain.
- Goodreads, a website where readers of books share their thoughts about them.

- Wikipedia, the free online encyclopedia made entirely of user-generated content, which against the odds has emerged as an example of the Internet doing something right, providing both reliable information and a valuable starting point for in-depth research.

It is just not possible to take the words of the bill and draw a line that includes Instagram while excluding Wikipedia. This is the inevitable consequence of trying to regulate all communication platforms without regard to their size, amount and sources of income, and purpose. If you aim at TikTok and hit Wikipedia instead, you are making a mistake.

HB47 attempts to penalize an entire communications medium because of the bad behavior of two or three companies. In so doing, it strangles the possibilities for a better Internet, and it harms those it is meant to protect.

II. CONSTITUTIONAL ISSUES

There are serious Constitutional issues with this bill. First and foremost, it evidently bars people—not just young people, but adults who are unable or unwilling to submit to age verification—from websites that offer nothing obscene. And obscenity is the dividing line for where age verification can pass Constitutional muster.[1] Likewise, the bill runs directly into the Commerce Clause of the United States Constitution. It imposes requirements on the activity of persons entirely outside the state of Alaska. Any platform outside of the state must still build the reporting and monitoring infrastructure to detect whether a user is covered. A resident of New York, accessing a platform hosted in Massachusetts, must sacrifice their anonymity to comply with a law that none of their elected representatives could have voted for. Because the law would have "the impermissible practical effect of controlling commercial activity wholly outside" Alaska, it goes beyond what the Commerce Clause can allow.[2]

In addition, the bill includes provisions that are sufficiently unclear that the law is open to being ruled void for vagueness. Consider the prohibition on "addictive features", which forbids any feature that "encourages or rewards a minor user's excessive or compulsive use of the platform or that exploits the psychological vulnerabilities of a minor user". What, exactly, is a "psychological vulnerability"? Most people are vulnerable to pictures of puppies and kittens; are websites forbidden from showing adorable pets to minors? How much use is "excessive", and when does use qualify as "compulsive"? Young people with deep religious convictions might check compulsively for a Bible quote of the day. *Any* feature that makes a site more user-friendly will increase the time spent on it; a feature that is entirely benign to 99% of minor users could contribute to compulsive behavior in the remaining 1%. This prohibition may *sound* good, but it provides no standard that is actually clear enough to follow.[3]

---

[1] See *Free Speech Coalition, Inc. v. Paxton,* 606 U.S. 461 (2025), where the majority and minority opinions agreed that "for fully protected speech, the distinction between bans and burdens makes no difference to the level of scrutiny" (internal quotation marks omitted). See also *Moody v. NetChoice, LLC,* 603 U. S. 707 (2024); *Brown v. Entertainment Merchants Assn.,* 564 U. S. 786 (2011); and *NetChoice v. Fitch,* 606 U.S. __ (2025), J. Kavanaugh concurring in denial of certiorari.

[2] *Healy v. Beer Institute, Inc.,* 491 U.S. 324 (1989).

[3] Per *Connally v. General Constr. Co.,* 269 U. S. 385, 391 (1926): "[A] statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess

Just this week, the Hawaii state legislature deferred their own bill that would have banned teens from social media. They cited "real Constitutionality concerns", with one representative calling it "very flawed".[4] The flaws of Hawaii's bill are the flaws of Alaska's too.

Moreover, the bill regulates how platforms must interact with users aged 13 to 17. This is contrary to the intent of Congress as codified into federal law, namely to regulate interactions with users younger than 13. The provisions of this bill could only become consistent with federal law if the Children's Online Privacy Protection Act were amended.

III. TECHNICAL IMPOSSIBILITIES

Because the bill's definition of "social media" sweeps so much more broadly than what those words mean in everyday speech, it makes demands that are simply not possible for platforms to meet. Consider provision 45.50.650(c)(2), which requires that a parent be able to "delete the minor's user account and all associated data". On Wikipedia, this would be flatly impossible. The software infrastructure is not built to allow it, and copyright law forbids it.[5] The bill would demand that *a free online encyclopedia* verify the ages of all its users and block all of them who are under 18: There is no other way to ensure compliance.

Moreover, because a "minor user" is defined to be anyone under 18 who "accesses or uses" a platform, even *reading Wikipedia* after 10:30 PM is forbidden. Why is a parental permission slip required for doing homework?

IV. THE HAZARDS OF DEMANDING AGE VERIFICATION

There is no way to verify the age of a user without obtaining information about that user. Compromising the individual's privacy is a logical necessity. And any compromise of privacy is a risk.

Last October, hackers broke into the service that the Discord platform used for age verification and stole the government-issued IDs of 70,000 people.[6] HB47 would not protect minors. On the contrary: It would put all citizens of Alaska at risk for identity theft.[7]

---

at its meaning and differ as to its application, violates the first essential of due process of law". And per *FCC v. Fox Television Stations, Inc.,* 567 U.S. 239 (2011): "Even when speech is not at issue, the void for vagueness doctrine addresses at least two connected but discrete due process concerns: first, that regulated parties should know what is required of them so they may act accordingly; second, precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way. [...] When speech is involved, rigorous adherence to those requirements is necessary to ensure that ambiguity does not chill protected speech."

[4] See the 5:08 PM discussion here: `https://www.youtube.com/watch?v=0Qa81c-_gT4`.

[5] See `https://en.wikipedia.org/wiki/Help:Delete_account`.

[6] A. Belanger, "Discord faces backlash over age checks after data breach exposed 70,000 IDs," *Ars Technica,* 9 February 2026.

[7] Rep. Alexandria Ocasio-Cortez recently put the issue in appropriately stark terms: politicians "are using kids as a smokescreen for what Big Tech lobbyists want: a national surveillance program to harvest our data with zero protections for people and their privacy." `@ocasio-cortez.house.gov` on Bluesky, 5 March 2026.

As with age verification, so too for parental consent. The blunt economic truth is that only platforms owned and run by Big Tech will be able to do it. A small player, like a nonprofit forum operated by volunteers, will be forced to quit the state entirely.

Denise Paolucci, co-owner of the blogging platform Dreamwidth Studios, has testified on this before a court of law:

> From my twenty-two year career in online Trust and Safety, I know that familial relationships are often far more complicated than conventional wisdom believes, and identifying which person is a minor's parent or guardian with legal decision-making authority is often a complex task. For instance, if a minor has two divorced parents who disagree about whether their minor child should be permittedt ohold an account on a website, the website must confirm the legal relationship between the parties and the minor involved, and determine which of the people at hand has the legal decision-making authority to provide sufficient parental consent. In a particularly contentious divorce, this can require a website to review divorce decrees, examine legal paperwork, and determine the authenticity and provenance of the documents supplied to them. Because someone who lives in [one state] may have obtained their divorce from any one of the thousands of courts across the United States, or even from another country, before moving to [that state], this would require us to become experts in authenticating and interpreting court documents from anywhere in the world to verify which parent has legal authority to provide parental consent. We do not have the capacity to perform this authentication, nor do we have the financial resources necessary to increase staffing to increase that capacity.
>
> [. . .]
>
> There is no national identity database that allows someone to verify a minor's identity, the legal relationship between a parent and a minor, or which parent has the authority to make binding decisions for a minor. There is no way to verify a user's identity beyond requiring the upload of government-issued identifying documents with corroborating photo or video confirmation, and many minors do not have photo ID. There is no way for a website to authenticate or verify that the documents uploaded for identity verification purposes belong to the person who is uploading them, that the person who controls the account is the same person who provided the identifying documents, or that the documents are legitimate and not a forgery. Disputes about the identity of an account holder, their age, or the legal relationship between them and the person claiming to be their parent are complex, time-consuming, costly to investigate and resolve, and unfortunately common. [A social media ban for youth] would only increase their number. We do not have the capacity to accept this additional support burden, nor do we have the financial resources necessary to increase staffing to increase that capacity.[8]

And, of course, any documents uploaded in such a process are potential targets for identity theft.

---

[8] Declaration of Denise Paolucci in Support of Plaintiff NetChoice's Motion for Preliminary Injuction, via `https://dw-news.dreamwidth.org/44429.html`.

V. COUNTERPRODUCTIVE PROHIBITION OF PERSONALIZATION

Section 45.50.680 forbids "content targeting minor users", i.e., the use of any technology to "select, recommend, rank, or personalize content for a minor user". Personalization can be a *good thing.* Platforms can recommend or prioritize content that is verified to be all-ages-appropriate. Conversely, downranking content is an essential part of protecting users, e.g., by filtering out scams and spam. Indeed, this Section would make it more difficult for platforms to shield minors against hate speech.

Suppose a platform implements a feature that detects when a user has been persistently active for a long interval of time and algorithmically insert a suggestion to go for a walk. Surely a good thing, no? But that would be personalization based on user data, and thus forbidden.

The restriction on using location data likewise leads to absurdities. An app for bird-watchers could not recommend to a minor pictures of birds in their vicinity. A website where people post restaurant reviews could not recommend restaurants nearby. Such restrictions serve no legitimate purpose.

VI. CONCLUSION AND ALTERNATIVES

Recent research suggests that among young people, *moderate* social-media use is associated with better mental health than either heavy use or no use at all.[9] Correlation is not causation; heavy social-media use can be a consequence of poor mental health (e.g., seeking distraction) rather than a cause. The world has gotten worse for teens in many ways, from the vanishing of "third spaces" to the failure of institutions to care about providing a livable future, and pointing the finger at social media alone is burying one's head in the sand.[10] The social and psychological factors at work are interrelated, complicated, and difficult to study:

> Despite a wealth of research on this topic, the evidence base is currently limited in several important respects. These include primarily cross-sectional work that does not warrant causal conclusions; use of small and homogeneous samples; failure to control for confounding factors (e.g., gender); and, in the case of social media research, a predominant focus on total time spent as opposed to *how* that time is used. Finally, with a handful of exceptions, research to date has also not distinguished between-person (i.e., stable differences between individuals) from within-person (i.e., situational changes within individuals) effects. This is critical because failure to do so can lead to erroneous conclusions regarding the presence, predominance, and sign of causal influences.[11]

This is not a good area in which to make blunt legal interventions. It is *certainly* not a

[9] B. Singh et al., "Social Media Use and Well-Being Across Adolescent Development," *JAMA Pediatrics* 180 (2026), 288–97.

[10] J. Severs, "Is Jonathan Haidt right about smartphones?" *Times Educational Supplement,* 3 September 2025.

[11] Q. Cheng et al., "How do social media use, gaming frequency, and internalizing symptoms predict each other over time in early-to-middle adolescence?" *Journal of Public Health* 48 (2026), 59–69.

topic where one bill should be wedged into another to make a Frankenstein's Monster of legislation. Complicated problems call for careful, flexible solutions.

I do not want to downplay the seriousness of young persons' use of social media. I have grave objections to the ways in which all of the largest social-media corporations behave, and I personally avoid all interactions with commercial social media to the fullest extent possible. I have opposed "Big Tech" for years, and I am writing out of concern that misguided attempts to regulate them will in fact entrench them. I wish to underline that, to address the issue, we must first diagnose it properly, and then we must go about solving it in a targeted and principled way. For example, talk of "social-media addiction" is well nigh ubiquitous, yet research suggests that portraying bad social-media habits as "addiction" makes those habits harder to break.[12] No one benefits when we boil our problems all down to "dopamine".[13]

There are better alternatives than the approach taken here. Multiple aligned pushes in the same direction can be more effective than a single blunderbuss of an intervention. We can put a tax on *all* targeted advertising. We can pass a strong privacy law that protects people of all ages, short-circuiting the toxic business models of giant corporations without "destroying the village in order to save it" by forcing platforms to gather data before deciding what amount of privacy they can offer. Consider a "youth center" model of reform, where we address the harms of the worst social-media platforms by giving teens better things to do on their phones. (Any minute spent playing a *Carmen Sandiego* game is a minute not spent on Instagram.) We can encourage independent and nonprofit social media by directing young people to platforms like Dreamwidth, Bluesky and Mastodon, platforms that aren't out to exploit them. We can educate parents about the safety features that already exist yet are under-utilized. As lawmakers, you can take a stand yourselves and cease using X and Meta, at once sending the message that we can live without these companies and broadening your own horizons about what the Internet has to offer.

Yours,
Blake C. Stacey, PhD
Co-moderator, TechTakes
Boston, MA
bstacey@mit.edu

[12] I. A. Anderson and W. Wood, "Overestimates of social media addiction are common but costly", *Scientific Reports* 15 (2025), 39388. https://www.nature.com/articles/s41598-025-27053-2.

[13] Nothing in brain science is as simple as a "pleasure chemical". As the neuropsychologist Vaughan Bell observed, "Traumatised war veterans, for example, show nucleus accumbens dopamine surges when they are reminded of the sounds of battle, something they find deeply aversive." See https://www.theguardian.com/science/2013/feb/03/dopamine-the-unsexy-truth.

TAXPAYERS PROTECTION ALLIANCE

April 8, 2026

The Honorable Kelly Merrick, Chair
The Honorable Forrest Dunbar, Vice Chair
Senate Community & Regional Affairs Committee
Alaska State Legislature
1500 W Benson Blvd
Anchorage, AK 99503

Chair Merrick, Vice Chair Dunbar and Members of the Committee:

On behalf of the millions of taxpayers and consumers we represent, the Taxpayers Protection Alliance (TPA) writes to express its concerns with House Bill 47 related to the bills proposal to require social media platforms to impose age verification on users. Despite its noble desire to protect children in the digital age, HB 47 would inadvertently create new risks for children and adults alike. This misguided legislation would endanger the privacy and data security of children and families across the state.

HB 47's fundamental flaw is its requirement that users of digital services submit to age verification, which requires users to submit a significant amount of sensitive personal information. This data would become 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. Given regular cybersecurity lapses, this mass collection of sensitive data would directly undermine the goal of ensuring children's safety in the digital world.

Children already face vast privacy dangers spurred by cybercrime. 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.

Unfortunately, the privacy dangers of HB 47 do not end there. Parents would be further required to give consent before their children are allowed to access social media platforms. Parental oversight of, and control over, their children's online lives is unquestionably best. However, the process outlined in the bill would compound risks to data security and privacy. Ensuring that the person claiming to be an underage user's parent is, in fact, that user's parents likely would require even more intrusive data gathering to prove both the identity of the parent and his or her status as the child's legal guardian.

Recent experience demonstrates the dangers of exposing 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 victim.[3]

[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.

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 recent 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 ostensibly privacy-protective age-verification mandates, such as those recently enacted in France, have exposed consumers to digital dangers.[5] Supreme Court Justice Alito put it best during the oral arguments in *Free Speech Coalition v. Paxton*: "There have been hacks of everything."[6]

Users widely understand the cybersecurity and privacy risks that accompany age verification mandates. In the United Kingdom, which recently enacted a broad age verification mandate in its Online Safety Act (OSA), vast numbers of users flooded app stores to download virtual private networks (VPNs) to avoid the mandate. In just the first few days after the OSA's provisions went into effect, VPN use skyrocketed. Proton VPN reported a 1,400-percent surge in new user registrations.[7] NordVPN reported a "1,000 percent increase in purchases," and many other VPNs reported increased user demand.[8]

Protecting children in the digital world, like protecting children in the physical world, is of the utmost importance. However, particularly when considering regulatory proposals to regulate novel digital technologies, it is critical to understand the unintended second- and third-order consequences that would flow from such proposals becoming law. Increasing experience has shown that age verification cuts directly against the goal of protecting children by exposing their personal information—and that of their families—to cybercriminals. TPA urges Alaska Legislators to double-down on a commitment to digital privacy—the only effective basis of personal privacy in a digital age—by rejecting age verification mandates or any other proposals that undermine safety.

Sincerely,

David Williams
President

[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.
[7] https://x.com/ProtonVPN/status/1948773319148245334.
[8] https://www.wired.com/story/vpn-use-spike-age-verification-laws-uk/.