March 17, 2026

House Committee on Judiciary Finance and Civil Law
Centennial Office Building
658 Cedar St.
Saint Paul, MN 55155

Re: HF 4138 - "Stop Harms from Addictive Social Media Act" (Oppose)

Dear Chair Scott, Chair Liebling, and Members of the House Committee on Judiciary Finance and Civil Law:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HF 4138. 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, HF 4138 introduces significant constitutional, operational, and privacy concerns that would negatively impact Minnesota residents and businesses.

HF 4138's method of designating covered services violates the First and Fourteenth Amendments.

HF 4138 covers online services based in part on whether they have the "primary purpose of posting and viewing information, comments, messages, images, or videos". Multiple federal courts have found this method of designating covered services to violate the First Amendment's prohibition on content-based speech restrictions and/or the Fourteenth Amendment's prohibition on vague laws.[3] As it is impossible to objectively determine whether a given "purpose" of an online service is its "primary" one, such services will not know whether the law applies to them. As an Arkansas federal court recently explained when invalidating a similarly worded statute, the law's framing "does not define... a term critical to determining

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

[3] *See, e.g.*, *NetChoice v. Jones*, No. 1:25-cv-02067 at *16-19 (E.D. Va. Feb. 27, 2026); *NetChoice v. Murrill*, No. 25-231, 2025 WL 3634112 at *86-88 (M.D. La. Dec. 15, 2025); *NetChoice v. Yost*, 778 F. Supp. 3d 923, 952-58 (S.D. Ohio 2025); *NetChoice v. Griffin*, No. 23-cv-05105, 2025 WL 978607 at *34-40 (W.D. Ark. Mar. 31, 2025); *SEAT v. Paxton*, 765 F. Supp. 3d 575, 594 (W.D. Tex. 2025); *CCIA v. Paxton*, 747 F. Supp. 3d 1011, 1032-24 (W.D. Tex. 2024).

which entities fall within its scope,"[4] thereby "leaving companies to guess whether their online services are covered."[5]

The above phrasing further violates the First Amendment by regulating speech based on a digital service's content. As a Virginia federal court recently explained, "creat[ing] an exemption for content preselected by the provider and not generated by users… favors provider-selected speech over user generated speech…. precisely the type of speaker preference the Supreme Court declared should be treated as content-based."[6] Several other federal courts have found such content-based regulation of digital service to be unconstitutional as well.[7]

The bill's requirements are not well-defined.

HF 4138 requires covered services to use "commercially reasonable"age estimation methods, but does not specify which methods are "commercially reasonable." Similarly, the bill covers account holders when the covered service "knows or should reasonably know the account holder is physically located in the state", without specifying when the service "should reasonably know" this information. It uses similarly vague language to define covered services' obligations to update their user age estimates, requiring that "reasonable means and reasonable efforts" be used but not clarifying which methods fall into this category. These subjective requirements do not provide covered services sufficient clarity to know if they are violating the law.

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

As the bill does not specify whether any given age assurance method is "commercially reasonable" and requires covered services to update some users' age estimates every 100 hours, covered businesses will effectively be forced to institute privacy-invasive age verification measures to ensure that they are in compliance. Requiring disputes about users' ages to be resolved by age verification compounds this problem. Furthermore, since the bill does not specify when a covered service "should reasonably know the account holder is physically located in the state", these services will be effectively forced to build location-based service tracking into their products to determine if users are in Minnesota. Likewise, the bill's parental consent requirements will inherently require companies to collect documentation capable of verifying a parental relationship, and such documents will inherently contain sensitive identifying information.

These requirements run contrary to the data minimization principles underlying federal and international best practices for privacy protection.[8] Requiring individuals to share sensitive personal information with third parties, including IDs or biometrics, can make recipients a

[4] *Griffin*, 2025 WL 978607 at *36.
[5] *Id.* at *37.
[6] *Jones*, No. 1:25-cv-02067 at *18 (cleaned up) (quoting *Reed v. Town of Gilbert, AZ*, 576 U.S. 155, 170 (2015)).
[7] *See, e.g.*, *Murrill*, 2025 WL 3634112 at *62; *Yost*, 778 F. Supp. 3d at 953; *Griffin*, 2025 WL 978607 at *22-24.
[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/.

prime target for identity theft, cyberattacks, or other data breaches.[9] Such dangers are far from hypothetical: several of the most devastating data breaches in recent years are directly attributable to age verification requirements.[10] Furthermore, government officials could access this sensitive data through enforcement inquiries and processes.

The more data a service is forced to collect, the greater risk it poses to consumer privacy and small business sustainability.[11] 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."[12]

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.[13] Though the intention to keep kids safe online is commendable, this bill undermines that initiative by requiring more data collection about young people.

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

The bill's broad definition of "addictive interface 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.'"[14]

---

[9] 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/.

[10] *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.

[11] 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.

[12] *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.

[13] *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.

[14] Am. Psychiatric Ass'n, Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision (2022).

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.[15] 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.[16] 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."[17]

To avoid restricting teens' access to information, HF 4138 should regulate users under 13 rather than 15 in accordance with established practices.

HF 4138's regulations apply to individuals less than 15. 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, if a 14-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 scope of covered users to be minors under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard.[18] 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.

The bill's private right of action would result in the proliferation of costly and questionable claims based on subjective criteria.

HF 4138 permits a private right of action for actual damages plus $10,000 in statutory damages where a violation was reckless or knowing. By creating a new private right of action, this measure would open the doors of state courthouses to plaintiffs advancing costly, time-intensive claims based on subjective criteria. The vague standards in this provision necessitate fact-specific inquiries that make courts reluctant — or unable — to dismiss claims until more facts can be gathered in the discovery phase. These new dynamics would significantly affect litigants' incentives. If defendants are routinely forced past the motion to dismiss phase and into full discovery, the cost of litigation itself becomes a coercive force, encouraging settlements unrelated to the strength of the legal claims. These costs would be passed on to individuals in Minnesota, disproportionately impacting smaller businesses and

[15] 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/.
[16] 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/.
[17] *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).
[18] *See* 15 U.S.C. § 6501(1).

startups across the state.[19] CCIA therefore recommends granting the state exclusive enforcement authority and adding a right to cure period to ensure that such costly litigation arises only when necessary.

* * * * *

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

Sincerely,

Megan Stokes
State Policy Director
Computer & Communications Industry Association

[19] Trevor Wagener, *State Regulation of Content Moderation Would Create Enormous Legal Costs for Platforms*, Broadband Breakfast (Mar. 23, 2021), https://broadbandbreakfast.com/trevor-wagener-state-regulation-of-content-moderation-would-create-enormous-legal-costs-for-platforms/.

Institute for family studies

16 March 2026

Dear Honorable Members of the House Judiciary, Finance, and Civil Law Committee:

I am a policy analyst at the Institute for Family Studies, which aims to advance the welfare of families and children through research, public education, and public policy. One of the ways we have pursued this goal is by developing and promoting policies that protect children online. To that end, our Institute strongly supports HF 4138. This bill is a constitutional, technically feasible solution that empowers parents to protect their children from social media companies that seek to exploit and addict children for the sake of profit.

Harms of Social Media and Addictive Feeds Are Well Established

Today, the exploitative design and harmful effects of social media are well-established. For kids and teens, especially, social media usage is not only linked to anxiety, depression, and sleep deprivation, it also exposes them to negative content that feeds suicidal ideation, eating disorders, body dysmorphia, and social comparison. Nevertheless, under existing federal law, minors are treated as digital adults once they turn 13. Moreover, existing federal statute lacks any meaningful mechanism by which to hold social media accountable for contracting with users they detect are under 13 (which they can), for failing to acquire parental consent for those under 13, or for addicting minors to algorithm-driven feeds that expose them to harmful content.

But, as is also well documented, the harms of social media do not cease when a minor turns 13. Sixteen-year-olds like Minnesota teen Carter Bremseth, who took his own like, was sextorted by a predator on Snapchat; 14-year-old girls have been algorithmically fed eating disorder content; and other teens, like South Carlolina's Mason Eden, have been encouraged to take their own life by pro-suicide content on TikTok.

This bill protects all teens and kids on social media by requiring platforms to acquire parents or legal caretakers—who are best positioned to care for their children—for any user they reliably detect is under age and forces them to terminate accounts if minor users cannot get parental consent.

Parental Controls Aren't Enough

According to a Pew Research Center, a majority of parents today monitor their teen's smartphone usage, such as reviewing browser or message history. Fifty-seven percent limit their teen's screentime, and 52% use parental controls. As of 2025, 86% of parents consider managing their child's screen time a priority when it comes to raising their kids. However, despite their efforts to monitor and limit their teen's digital activity, 9 in 10 parents remain worried about their children's online safety.

The Future Is Family
P.O. Box 1502 Charlottesville Virginia, 22902
434-326-7583 | michael@ifstudies.org
www.ifstudies.org

This is hardly surprising. Social media companies have long used parental controls and screen time settings as a kind of window dressing to appease the public eye, when in fact their settings do not ultimately deter users from staying engaged with their platforms. For example, TikTok, the second most popular social media platform used by teens, created a tool that they knew would do nothing to actually decrease app usage. It was simply a ploy to earn public trust. Meta, too, knows that Instagram shows more eating disorder content to teens already struggling with body image issues.

This bill puts the power back into parents' hands by prohibiting social media companies design their platforms in ways that do not addict or advertise to children and by requiring platforms to go through parents first before children use platforms instead of simply providing parental controls after the fact.

Constitutional Contracts & Parental Consent

Ultimately, this bill is about contracts, not content. In every other industry, companies and corporations are required to get parental consent before entering into a contract with a minor. This restriction exists regardless of whether a particular good or service is deemed good or bad for a minor. Rather, it exists to protect children from being taken advantage of and from entering into decisions whose risks or consequences they cannot fully grasp due to their development stage.

However, this has not been the case when it comes to social media. For years, these companies have been permitted to enter into complex contracts (e.g. terms of services and privacy policies) with minors. This bill fixes this problem by explicitly requiring social media companies to require parental consent before minors can agree to or be held accountable to their terms of services.

As such, this bill is constitutional and poses no threat or burden to first amendment rights. This bill does not prohibit any child from accessing social media platforms or the content therein. So long as they have their parent's consent, they are free to use whatever they please. Moreover, this bill does not expose adults to any significant burdens on free speech or put children's privacy at risk because it utilizes data these companies already collect and have long used to accurately predict user's age.

Conclusion

When it comes to raising kids, parents need help—especially online. By applying real world commonsense to the digital world and putting power—*real power*—back into parents' hands, HF 4138 helps parents and makes the online world safer for their children. We strongly urge you to support and advance this bill.

Respectfully,

Jared Hayden
Policy Analyst, Family First Tech Initiative, Institute for Family Studies

Testimony of Clare Morell, Author of *The Tech Exit: A Practical Guide to Freeing Kids and Teens from Smartphones* in support of Minnesota HF 4138

Executive Summary:

- The design of social media is inherently addictive, especially to the developing brains of minors and is causing an epidemic of addiction and mental illness among America's youth. Social media's business model is addicting our kids.
- The current age limits, parental controls, and screen time limits that social media companies hold out as the solution to protecting kids are woefully ineffective. Parental controls are a myth, parents are not in control, the company's algorithms are. And screen time limits don't work with an incredibly addictive product -- even a short amount of time spent on these apps is addicting to a child's developing brain.
- Parents on the frontlines need help from lawmakers. SHASM critically puts parents in control over children getting on to social media and helps parents beat the collective action problem of social media. Currently, there is no parental consent or age verification required to get a social media account, so even if a parent is trying to keep a child off of social media, it's incredibly difficult to enforce. The social pressures also make it difficult for individual parents be the "first mover" to resist social media for their kids. Laws like SHASM can help set a new collective norm to limit social media for minors under 16 that supports parents in their individual decisions with their children. By requiring **age estimation**, SHASM also puts real teeth in age limits and parental consent. If parents do consent, SHASM still provides important protections against addictive exploitation, undermining social media's predatory business model towards kids.

I. SOCIAL MEDIA AND THE YOUTH MENTAL HEALTH CRISIS

Since 2010, the rates of anxiety, depression, self-harm, and suicide among teens have spiked. In the last decade, from 2010 to 2020, emergency room admissions for self-harm injuries among 10- to 14-year-old girls quadrupled.[1] A four-fold increase. The 2023 CDC Youth Risk Behavior Survey found that 1 in 3 high school girls had seriously considered taking her own life in the past year. One in three.[2]

Social media use is *causing* these declines in mental health and increases in self-harm and suicidality. As Jonathan Haidt has explained, "Between 2010 and 2015, the social lives of American teens moved largely onto smartphones with continuous access to social media.

[1] The Anxious Generation, The Evidence, March 2, 2024,https://www.anxiousgeneration.com/research/the-evidence

[2] CDC, U.S. Teen Girls Experiencing Increased Sadness and Violence, February 13, 2023, https://www.cdc.gov/media/releases/2023/p0213-yrbs.html#:~:text=Nearly%201%20in%203%20(30,Black%20youth%20and%20White%20youth.

. . The first generation of Americans who went through puberty with smartphones . . . in their hands became more anxious, depressed, self-harming and suicidal."[3]

A. The harms are driven by addictive design.

Children's and teen's brains are particularly vulnerable to the design of social media. The regions of the brain associated with social rewards undergo significant development during adolescence, as the brain's dopamine receptors multiply between the ages of ten and twelve. This is a normal part of adolescent development that helps children bond with their peers. Social media takes this natural process and hijacks it with an environment built on teens holding themselves out to the world for review and judgment, for instant feedback and gratification, with metrics for constant comparison with others—the perfect recipe for teens to become anxiously addicted to checking their phones.[5]

Social media further generates this addiction by using design features, like constant notifications, "likes", daily streaks, infinite scroll, and feeds customized by recommendation algorithms that learn what a user likes and continues to give him more of the same content to keep him hooked, all of which stimulate the brain to release dopamine. Dopamine is a neurotransmitter involved in the brain's reward system that gives the brain a little burst of pleasure. Dopamine, however, doesn't create satisfaction or lasting pleasure; it only produces "wanting" so the user will repeat that action again. Brain imaging studies indeed show that the impact of social media on the structure of the brain resembles that of a highly addictive drug, like cocaine.[4]

The huge exposure of children and adolescents to pornography and to obviously harmful material such as videos advocating dangerous "challenges" or self-harm on social media attracts much attention, and rightly so. But the science tells us that constantly drawing children's attention back to these apps, even to superficially "harmless" content, inflicts harm on children's developing brains. In 2023, University of North Carolina researchers published a study that found that sixth and seventh grade students who checked social media platforms (Facebook, Instagram, and Snapchat) multiple times throughout the day, to say nothing about the content viewed or amount of time spent on the apps, demonstrated divergent brain development over time.[5]

---

[3] Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Child Is Causing an Epidemic of Mental Illness* (New York: Penguin, 2024), 44-45.

[4] Christian Montag et al., "Internet Communication Disorder and the Structure of the Human Brain: Initial Insights on WeChat Addiction," *Scientific Reports* 8 (2018), doi.org/10.1038/s41598-018-19904-y; Fuchun Lin and Hao Lei, "Structural Brain Imaging and Internet Addiction," in *Internet Addiction: Neuroscientific Approaches and Therapeutical Interventions*, ed. Christian Montag and Martin Reuter (New York: Springer, 2015), 21–42.

[5] Maria T. Maza et al., "Association of Habitual Checking Behaviors on Social Media with Longitudinal Functional Brain Development," *JAMA Pediatrics* 177, no. 2 (2023): 160–67, doi.org/10.1001/jamapediatrics.2022.4924.

While other bills may take aim at specific harmful *content*, SHASM takes aim at the core problem of addictive use of social media by children.

B. Social Media companies *want* to addict your child.

Addiction is not an accidental consequence; it is the goal that platforms have intentionally pursued. Social media appears "free" to your child—but your child's time, attention, and data is the product being sold. More hours with eyes glued to the screen means more time for advertisements. The user is the product. That's social media's business model. Sean Parker, the founding president of Facebook, has since explained that when Facebook was being developed the objective was: "How do we consume as much of your time and conscious attention as possible?"[6]

New internal documents have come to light through litigation, showing these companies intentionally addicted our kids. One internal Meta employee message exchange compares Instagram to drugs and slot machines. "Oh my gosh yall IG is a drug," "Lol, I mean, all social media. We're basically pushers."[7] Internal TikTok documents, likewise, document that the company is well aware that their users "think the platform is addictive." When TikTok designers proposed modifications to reduce addictive use of TikTok, senior management was only willing to consider changes that would result in no more than a 5% drop in "stay time."[8]

Social media companies also want to addict your child because they know that once children get hooked on a specific platform, they tend to stick with that platform on into their adult years when they spend more and are worth even more to advertisers. The younger a platform can addict a user, the longer they can profit off of that person over the course of their lifetime. An internal Meta report states, "the young ones are the best ones" in explaining why young users have greater long-term retention for the company in using their products.[9]

II. EXISTING "PROTECTIONS" ARE INEFFECTIVE

A. Age limits are a sham.

Despite hollow promises to the contrary, social media platforms have little interest in keeping underage minors off their platforms. Rather, for the reasons mentioned above, these companies are in a race to the bottom for our children. Although age 13 is

---

[6] Mike Allen, "Sean Parker unloads on Facebook: 'God only knows what it's doing to our children's brains'", Axios, November 9, 2017, available at: https://www.axios.com/2017/12/15/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792

[7] MDL. No. 3047, Amended Exhibit 74, https://storage.courtlistener.com/recap/gov.uscourts.cand.401490/gov.uscourts.cand.401490.2648.39.pdf

[8] *Kentucky v. TikTok* Compl. ¶¶ 126, 146, 203, 210.

[9] MDL. No. 3047, Amended Exhibit 313, https://storage.courtlistener.com/recap/gov.uscourts.cand.401490/gov.uscourts.cand.401490.2648.42.pdf

commonly the minimum age used by social media platforms in the U.S. (because according to the federal law, COPPA, companies cannot collect data on children under the age of 13 without parental consent) nearly 40% of children ages 8–12 use social media. [10] That is nearly half of pre-teens! The companies are not enforcing their own age limits and have been resistant to implement more robust age-verification processes. All a child needs to do is enter a birth date (easy for kids to lie about) and check a box to agree to the terms and services. A parent may never know, since no parental consent is required.

B. Parental controls are ineffective.

Social media companies have worked to convince parents that if they just enable the parental controls on their apps, their children will be safe. Instagram, along with many of the other major social media platforms like Snapchat, TikTok, and Discord, offers "parental supervision" tools, but in all cases, the teen has to accept the supervision and can cancel it at any time (though the parent will get a notification if it's canceled). And even that supervision is extremely limited. The controls mainly allow the parent to set daily time limits and breaks and manage privacy settings, but the parent has no insight into posts in the child's feed or the content of messages sent and received. If parents can't meaningfully oversee their children's online activity and communications, and if account restrictions can't truly be locked in by a parent, then the idea that these are parental controls is a myth. Platforms essentially put teens, with their underdeveloped brains, in the driver's seat when it comes to their experience on social media.

Not to mention that parental controls are meaningless when kids can and do create accounts without their parents' knowledge. Even worse, some of the most dangerous apps, like Snapchat, TikTok, and Discord, all block external third-party controls that a parent may install from accessing the data inside the apps. The reality is the companies' addictive algorithms determine a child's online experience, not the parents.

C. Screen time limits are not enough.

Even if kids couldn't get around parent-set time limits (which they can), the limits still wouldn't beat the addiction mechanisms built into social media. With an addictive product, time limits are no match. The negative effects from social media's constant dopamine hits do not occur only when someone is spending too much time on it, rather the compulsive checking behavior social media induces, regardless of time spent, causes divergent brain development, as the 2023 UNC study mentioned above shows.

Time limits also don't map on to a child's mental or emotional time spent on the platform. Even if a child is only allowed on social media for thirty minutes a day, that brief exposure can dominate their mental space for the rest of the day. Because of the

[10] Rideout, V., Peebles, A., Mann, S., & Robb, M. B. (2022). Common Sense census: Media use by tweens and teens, 2021. San Francisco, CA: Common Sense.

built-in social metrics, children are constantly thinking about the next time they can get on the app to see what "likes" they may have gotten or new content friends might be posting. Kids carry the virtual world with them long after they "leave" it. This is because once they leave the app, the brain does not return to a baseline level of dopamine, it actually plunges into a dopamine deficit state, which creates the constant craving to go back on. The time limit is never enough.

D. An existential threat.

The harms social media are causing to America's youth go much deeper than the mental health epidemic of spiking rates of teen anxiety, depression, and self-harm. These are real concerns but they are only symptoms of a much greater spiritual disease afflicting American childhood—social media habituates children towards an inhumane way of life.

The character traits that are adaptive for the world of social media are maladaptive for the real world. Social media creates dependence and addiction, instead of independence and freedom. It rewards and celebrates self-focus and self-expression rather than responsibility and service to others. It is a world built on metrics, "likes," reshares, and superficial connections instead of friendship, trust, and conversation. It wires children for consumption instead of production.

These results are the exact opposite of what parents want for their children and to what is best for our nation. The endurance of our self-governing republic depends on a virtuous, flourishing citizenry, men and women will be contributing members of society, who will make their country a better place, and who are qualified to serve as leaders. The social media companies are working to form a different kind of person. Their apps are designed to overpower human self-control and turn our children into unthinking, dopamine-addicted *users*.

We are at a crisis point. Parents are in a competition with these Big Tech companies, and whoever wins that competition is going to determine what the future citizens of our country are like, and therefore what kind of nation we become. The souls of our children and the soul of our nation is at stake. We need lawmakers to help parents win this fight.

III. PASS SHASM

A. SHASM critically puts parents in control over children getting on to social media and helps parents beat the collective action problem of social media.

SHASM requires social media platforms to terminate the accounts of users determined to be under age 16 unless and until they obtain "verifiable parental consent," as defined in COPPA. This puts parents back in the driver's seat over if and when a child gets to create a social media account.

Also, because the COPPA requirement for "verifiable parental consent" has proven sufficient to discourage at least most major social media platforms from providing accounts for minors who admit to being under age 13 at all, the best-case scenario is that under SHASM, this requirement would lead the companies to set a new age limit of 16. And therefore, SHASM also could help solve the "first mover" or collective action problem of social media, where parents have felt socially pressured into letting their kids on because every other kid has an account.

B. By requiring **age estimation**, SHASM puts real teeth in age limits and parental consent that can withstand constitutional challenge.

The industry's practice of accepting children's "check-box" lies about their ages has betrayed our children. Recently, several states have passed laws requiring some form of "age verification" before an account can be opened. New technologies promise that age verification can be done anonymously, but some civil libertarians on both the left and right have expressed doubt about that anonymity, and some courts have held age verification requirements unconstitutional because of their potential impact on adults.

SHASM takes a different approach. SHASM requires the large social media companies to use the same AI power they deploy to profile, addict, and sell your child, to estimate the ages of users, identify children, and close their accounts—unless and until those companies obtain concrete, verifiable consent from a parent. No form of identification is required from the user. Their business model is targeted advertising, so the companies know who their users are. Children's online behavior patterns are distinctive, and they can't successfully act like adults for long. The major social media companies have said publicly that they *can* do this; SHASM would require that they *do* do it.

C. If parents do consent, SHASM still provides important protections against addictive exploitation.

Some parents want their children to have social media accounts, but no parent wants their child addicted. If parents do consent, SHASM respects that decision, while still providing important protections. SHASM prohibits presenting specific and purposefully addictive interface features on children's accounts, and SHASM prohibits those companies from using their recording and AI analysis of your child's online behaviors to craft a personalized addictive feed.

D. SHASM is one important line of defense for our children.

Legislatures should certainly enact high barriers to keep young people off of pornography websites, as the Supreme Court recently approved in its *Free Speech Coalition v. Paxton* decision this year. But such laws will not address the harms to our children of *addiction* to social media. SHASM provides a new and important line of defense for our children against the determined efforts of social media companies to addict our children and sell their attention for profit.

Amy Bos
Vice President Government Affairs, NetChoice
Washington, DC 20005

NetChoice
Defending Free Speech and Free Enterprise Online

Minnesota, Stop Harms from Addictive Social Media Act

TESTIMONY IN OPPOSITION

March 17, 2026

Minnesota Legislature
House Judiciary Committee

Dear Members of the House Judiciary Committee:

On behalf of NetChoice, a trade association working to make the internet safe for free enterprise and free expression, I write to express our strong opposition to House Bill 4138. Among other sweeping provisions, the bill mandates age estimation for all Minnesota account holders, requires verifiable parental consent before any minor aged 15 or younger can create or maintain an account, bans an overbroad set of features the bill characterizes as "addictive," and creates a sweeping private right of action with statutory damages of $10,000 per knowing or reckless violation.

NetChoice respectfully asks that you **oppose** the legislation as it:

- Fails to protect a single citizen from harm
- Puts minors's sensitive data at risk
- Violates the 1st Amendment of the US Constitution

We share the sponsor's genuine concern for the wellbeing of Minnesota's children online. NetChoice members have taken teen safety seriously and in recent years have introduced numerous new features, parental control tools, and platform-level protections to better empower families. We welcome continued dialogue with the Legislature on these issues. However, effective child safety policy must be narrowly tailored, technically feasible, and constitutionally sound. HF 4138 falls short on all three counts.

HF 4138 Puts Minors' Sensitive Data at Risk

This bill is ostensibly designed to protect children, but its age estimation and parental consent mandates would, in practice, require platforms to collect far more sensitive information about Minnesota users — including children — than they collect today.

The bill's age estimation requirement in Subdivision 2 creates a cascading set of algorithmic obligations. Once an account holder accumulates 25 hours of use within a six-month period, a covered platform has 14 days to estimate the user's age with 80% confidence. At 50 hours, that confidence threshold rises to 90%. Platforms must then update their estimates after every additional 100 hours of use — or whenever they apply any data analytics or AI to update any other demographic characteristic of a user, whichever comes first. This last provision is particularly significant: it effectively mandates near-continuous demographic profiling of all Minnesota account holders, the very outcome child privacy advocates seek to prevent.

To meet these confidence thresholds, platforms will face strong incentives to collect and retain the kinds of identifying data — device fingerprints, behavioral signals, and ultimately government-issued identification — that can be used to estimate age with the required statistical precision. The bill's verifiable parental consent requirement, incorporating the COPPA standard under 15 U.S.C. § 6501(9) and 16 C.F.R. § 312.5, compounds this problem. Obtaining verifiable parental consent at scale will require platforms to collect, store, and process sensitive identity documentation from both minors and their parents. Large-scale mandatory collection of highly sensitive personal and governmental identification data dramatically increases the risk that this information will be captured in data breaches or misused by bad actors — the very harms Minnesota families most fear.

In short, the bill would mandate the creation of detailed identity dossiers on Minnesota families in the name of child safety.

HF 4138 Violates the 1st Amendment of the US Constitution- At Least Twice Over

This bill presents at least two independent First Amendment violations. First, it infringes on the rights of users to receive protected expression without first having their age "estimated" by the platform and, if determined to be a minor, securing parental consent. Second, it infringes on the rights of platforms to disseminate their own "distinctive expressive offering" to users without engaging in invasive age estimation and verification processes.

Age Estimation, Verification, and Parental Consent Requirements Are Unconstitutional

Restrictions on the access to and enjoyment of speech are rarely permitted. Indeed, restrictions are permitted only for certain categories of speech, and the Court has been careful to articulate such categories as obscenity, incitement, true threats, and fighting words. But the government cannot create new categories of unprotected speech to solve some perceived social harm. *Brown*, 564 U.S. at 792. And, as *Packingham* recognized, social media is home to troves of protected, valuable speech. 582 U.S. at 105.

When the government has attempted to restrict access to speech through requirements for speakers to "determine" or "verify" the age of audience members, the Supreme Court routinely struck them down. Such restrictions impermissibly chill speech by dissuading otherwise willing speakers and listeners from participating. The government may not impose barriers as a precondition to speak or receive the speech of others. *See Reno v. ACLU*, 521 U.S. 844, 855-857 (1997); *Ashcroft v. ACLU*, 542 U.S. 656 (2004).

Similarly, the Supreme Court also invalidated parental consent requirements to access lawful speech. *Brown*, 564 U.S. 786 (2011).

While HF 4138 does not purport to prevent access to social media websites outright, it *does* restrict access to the website's "distinctive expressive offering." *Moody v. NetChoice*, 603 U.S. at 738. That offering is protected expression, and the government may not prevent access to that offering any more than it could dictate how the *New York Times* or *Wall Street Journal* arrange articles in their newspapers.

Restrictions on Dissemination of Lawful Speech are Unconstitutional

Distinct from the First Amendment injury HF 4138 inflicts on the viewers, readers, and users of social media websites, the law inflicts a separate injury on *websites* because it prevents them from freely offering their own "distinctive expressive offering."

The bill would make it unlawful for social media websites to offer content that is "recommended, selected, or prioritized" to users without either determining the user is an adult or obtaining parental consent for minors. This restriction prevents the exercise of editorial discretion. The judgment about what content to display "rest[s] on a set of beliefs about which messages are appropriate" to prioritize and display to users is expressive. And the government does not have the authority to alter those decisions merely because it believes it would make better choices. *Id*. at 738.

The Supreme Court's decision last term in *NetChoice* emphatically held that the personalized feeds available on social media websites like Facebook and YouTube are protected expression under the First Amendment. Because HF 4138 would prevent the exercise of editorial discretion by prohibiting the use of these personalized feeds, it is unconstitutional.

HB542's Private Right of Action Invites Costly, Abusive Litigation

Beyond its constitutional and privacy deficiencies, the bill's enforcement mechanism in Subdivision 8 will generate substantial harm of its own.

The bill creates a private right of action available to any child or parent for declaratory relief, injunctive relief, general and special damages, attorney fees — and, critically, $10,000 in statutory damages per knowing or reckless violation. It also provides for punitive damages where a "consistent pattern" of reckless or knowing conduct is established. The statute of limitations is tolled until the child turns 18, meaning platforms face liability exposure lasting years or even decades after the alleged conduct.

This combination of provisions will invite opportunistic litigation untethered from any demonstrated harm to specific children. The bill's novel age estimation requirements — built around concepts like "80% confidence" and "reasonable means and reasonable efforts" — are technically complex and inherently ambiguous. Courts and juries will be asked to adjudicate difficult algorithmic and engineering questions without clear legislative standards to guide them. Rather than incentivizing better outcomes for children,

this litigation mechanism will incentivize platforms to over-collect and over-retain user data in order to defend against lawsuits, further undermining the very privacy interests the bill purports to advance.

The Legislature should, at minimum, strip the private right of action from this bill and rely instead on targeted, consistent, and expert-informed enforcement by the Attorney General under Section 8.31 — authority the bill already provides.

* * * * *

NetChoice and its members are committed to making the internet safer for Minnesota children. We have supported parental control tools, time management features, digital literacy initiatives, and industry-led protections designed to keep young users safe. We recognize that more can and should be done, and we genuinely welcome the Legislature's continued engagement on this issue.

But good intentions do not insulate legislation from constitutional scrutiny. Because Section HF 4138 would compromise the data security of Minnesota families, restrict constitutionally protected speech and editorial judgment, and unleash a wave of litigation that would harm rather than help the children it claims to protect, we respectfully urge the committee to oppose the bill as written.

We offer ourselves as a resource to discuss any of these concerns in greater detail and appreciate the opportunity to present our views on this important matter. Thank you again for the opportunity to provide the committee with our thoughts on this important matter.[1]

Sincerely,

Amy Bos
Vice President of Government Affairs
NetChoice
NetChoice is a trade association that works to make the internet safe for free enterprise and free expression.

[1] The views of NetChoice expressed here do not necessarily represent the views of NetChoice members.

March 16, 2026

The Honorable Peggy Scott
Co-Chair, Minnesota House Committee on Judiciary Finance and Civil Law
658 Cedar Street
St. Paul, MN 55155

The Honorable Tina Liebling
Co-Chair, Minnesota House Committee on Judiciary Finance and Civil Law
658 Cedar Street
St. Paul, MN 55155

RE: TechNet opposition to HF 4138

Dear Co-Chair Scott and Co-Chair Liebling:

I am writing in respectful opposition to HF 4138. TechNet appreciates the bill's focus on the important goal of protecting children online. Our member companies invest heavily in safety tools, parental controls, and age-appropriate experiences for younger users. However, HF 4138 raises substantial concerns because it would expand data-processing obligations and impose an unusually punitive enforcement framework that is likely to generate litigation without producing better safety outcomes for children. The bill also contains additional concerns related to definitions and other substantive provisions that we understand are more appropriately the subject of discussion in the Commerce Committee.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

<u>HF 4138 raises significant privacy concerns by compelling sensitive age-related inference and parental-account data handling</u>
Although the bill states that a covered platform has no duty to collect additional information beyond what it already retains, it still requires platforms to estimate age after specified usage thresholds and to treat users as children unless the platform can conclude with 80 percent confidence and later 90 percent confidence that the user is older than 15. In practice, this creates pressure to engage in

sensitive age-related inference and to repeatedly reassess users over time. The bill also requires verifiable parental consent before creating or maintaining a child account or changing that account's terms, and it adds a documentation-retention requirement tied to proving that consent was obtained. Even where intended to protect minors, these requirements create privacy and data-governance concerns by pushing platforms toward more intensive age and family-status determinations than many services otherwise would make.

The bill also prescribes a parental-access architecture that is likely to increase data handling and account-management complexity. As part of obtaining parental consent, a platform must prominently offer the parent a separate-password option that enables monitoring of time spent, daily and weekly limits, and time-of-day restrictions. While parental tools can be valuable, the state should be cautious about requiring a particular model that may necessitate additional credentialing, documentation, and account-linkage practices, all of which carry privacy and security implications.

The bill's enforcement and penalty structure is extraordinarily aggressive and invites private litigation

The bill establishes enforcement mechanisms for child-account regulations and, as drafted, creates a framework designed to support extensive private litigation. Private right of action models with statutory damages, punitive damages, and fee shifting risk benefiting lawyers more than families and diverting resources away from investment in safety tools and compliance efforts.

That concern is particularly acute here because HF 4138 pairs complex operational duties such as age estimation, parental consent workflows, privacy-default requirements, and content/ad-delivery restrictions with civil law consequences. When a bill imposes liability in an area involving evolving technologies, probabilistic assessments, and judgment-laden implementation questions, broad private enforcement is especially likely to produce costly and inconsistent litigation. Enforcement of complex technology rules is better handled by appropriate regulators exercising discretion and focusing on genuine bad actors, rather than by a sweeping litigation model layered on top of ambiguous and untested compliance standards.

TechNet also has concerns with the bill's definitions and other substantive provisions

In addition to the privacy and penalty issues discussed above, TechNet has concerns with several defined terms and other operative provisions in the bill, including the breadth of the definitions governing covered platforms, covered users, "addictive interface features," and advertising-related restrictions. Those issues raise separate questions about scope, clarity, and operational feasibility. We understand those aspects of the bill are best addressed in the Commerce Committee, and we appreciate the opportunity to continue that conversation.

TechNet shares the Legislature's commitment to protecting children online, but HF 4138 adopts a prescriptive and punitive framework. A more effective approach would build on existing federal law, preserve parental choice without extensive data collection requirements, and allow platforms to continue improving safety outcomes without imposing unworkable age-estimation mandates, rigid product-design restrictions, and sweeping litigation risk.

For these reasons, TechNet respectfully opposes HF 4138. Thank you for considering our concerns, and please feel free to reach out if you have any questions.

Sincerely,

Ninia Linero
Executive Director, Illinois and the Midwest
TechNet