March 1, 2023

House Commerce Finance and Policy
Attn: Simon Brown, Committee Administrator
100 Rev. Dr. Martin Luther King Jr. Blvd.
St. Paul, MN 55155-1298

Re: HF 1503 - "Social media algorithms that target children prohibited." (OPPOSE)

Dear Chair Stephenson and Members of the Commerce Finance and Policy Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HF 1503. CCIA is an international, not-for-profit trade association[1] representing a broad cross-section of communications and technology firms. While CCIA shares the Committee's concern and agrees more work can and must be done to study the potential implications of automated systems and related technology, HF 1503 is not the solution.

1. Automated decision-making is complex. The use of this technology can generate both benefits and drawbacks. Since these technologies are nuanced, there could be a variety of unintended consequences if one were to regulate them in haste.

The span of automated decision-making is elaborate and often misunderstood.[2] At its core, automated decision-making is simply a set of techniques that can be used for doing tasks that would otherwise be accomplished manually or using traditional, non-AI technology. These technologies are data-driven and can efficiently process massive amounts of data to create gains in productivity and accuracy and support technological and scientific breakthroughs.

Automated decision-making models touch almost every aspect of our day-to-day activities. This includes filtering spam emails, using ride-share apps, online shopping, plagiarism scans, using smartwatches to track a workout, monitoring online test taking, and pre-authorizing medical insurance before a visit. It is important to note that digital services also use these technologies to protect users, such as filtering out dangerous or illegal conduct or content on their platforms. By prohibiting these businesses from using these types of technologies to remove this harmful content, the bill unintentionally undermines their efforts to protect minors who could become susceptible to this type of dangerous content.[3]

---

[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] *See generally* Mike Masnick, *The Latest Version Of Congress's Anti-Algorithm Bill Is Based On Two Separate Debunked Myths & A Misunderstanding Of How Things Work*, Techdirt (Nov. 11, 2021), https://www.techdirt.com/2021/11/10/latest-version-congresss-anti-algorithm-bill-is-based-two-separate-debunked-myths-misunderstanding-how-things-work/.

[3] *See generally* Elizabeth Ruiz, *Artificial Intelligence Is Helping to Protect Your Children Online*, ABC Action News (Feb. 9, 2023), https://www.abcactionnews.com/news/national/artificial-intelligence-is-helping-to-protect-your-children-online.

Ambiguous and inconsistent regulation at the state or local levels would also undermine business certainty, creating significant confusion surrounding compliance. This type of regulatory patchwork may deter new entrants, harming competition and consumers. While we share the concern with the Committee that it is imperative to keep children safe online, we must also strike the correct balance to avoid stifling the use of technology when organizations are looking to use automated decision-making as an essential tool to help their businesses and the users on their platforms. We urge Committee members to study both the benefits and drawbacks of automated decision-making technologies and to engage with practitioners and stakeholders to support the ongoing development of practicable solutions.

2. There are several ongoing studies at the national level aimed at understanding how to balance the capabilities and risks of automated decision-making. These studies are intended to inform appropriately tailored and impactful regulation of such systems.

The automated decision-making systems that lawmakers seek to regulate are complex and warrant adequate understanding to reach intended outcomes appropriately. For example, the National Artificial Intelligence Initiative (NAII) was established by bipartisan federal legislation enacted in 2021.[4] The NAII is tasked with ensuring continued U.S. leadership in AI R&D while preparing the present and future U.S. workforce to integrate AI systems across all sectors of the economy and society. Importantly, NAII is doing so in partnership with academia, industry, non-profits, and civil society organizations. Most recently, the U.S. Congress passed legislation to create a training program to help federal employees responsible for purchasing and managing AI technologies better understand the capabilities and risks they pose to the American people.[5]

The National Institute of Standards and Technology (NIST) also launched the AI Risk Management Framework (RMF)[6], an ongoing effort aimed at helping organizations better manage risks in the design, development, use, and evaluation of AI products, services, and systems. The draft of the AI RMF was just released in January 2023.[7] The NIST National Cybersecurity Center of Excellence[8] is also leading federal regulatory efforts to establish practices for testing, evaluating, verifying, and validating AI systems.

The deliberate, thoughtful, and bipartisan fashion in which leaders at the federal level are approaching the wide variety of issues associated with automated decision-making is encouraging. These ongoing studies by national experts should signal the complexity of the issue. Lawmakers should wait for and review forthcoming best practices by technical experts to help inform the development of national standards and regulations.

[4] National Artificial Intelligence Initiative Act of 2020, Pub. L. No. 116-283, § 5001-5501, 134 Stat. 4523-4547 (2021).
[5] AI Training Act, Pub. L. No. 117-207, 136 Stat. 2238 (2022).
[6] NIST, *AI Risk Management Framework*, https://www.nist.gov/itl/ai-risk-management-framework (last accessed Feb. 24, 2023).
[7] NIST, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[8] NIST, *National Cybersecurity Center of Excellence, Mitigation of AI/ML Bias in Context*, https://www.nccoe.nist.gov/projects/mitigating-aiml-bias-context (last accessed Feb. 24, 2023).

3. As drafted, HF 1503 may actually put Minnesotans at greater risk of harm, including children that the bill seeks to protect.

HF 1503 provides several examples of how to obtain verifiable consent, however, this raises questions about whether such unspecified verification mechanisms would conflict with data minimization principles and other consumer data privacy protection measures. CCIA is concerned that businesses may be forced to collect age verification data, which would paradoxically force companies to collect a higher volume of data on users.[9] Businesses may be forced to accumulate personal information they do not want to collect and consumers do not want to give, and that data collection creates extra privacy and security risks for everyone. This mandated data collection would include collecting highly sensitive personal information about children, including collecting and storing their geolocation to ensure they do not reside outside of the state when confirming that they are of age to be using these services.

When the federal Communications Decency Act was passed, there was an effort to sort the online population into children and adults for different regulatory treatment. That requirement was struck down by the U.S. Supreme Court as unconstitutional because of the infeasibility.[10] After 25 years, age authentication still remains a vexing technical and social challenge.[11] Though the intention to keep younger users safe online is commendable, this bill is counterproductive to that initiative by requiring more data collection about young people and their parents. California recently enacted legislation that would implement similar age verification measures which is currently being challenged for similar reasons.[12] CCIA recommends that lawmakers permit this issue to be more fully examined by the judiciary before burdening businesses with legislation that risks being invalidated.

4. The bill lacks narrowly tailored definitions.

As currently written, the bill *indirectly* defines a child as anyone under 18. Due to the nuanced ways in which children under the age of 18 use the internet, it is imperative to tailor such treatments to respective age groups appropriately. For example, if a 16-year-old is conducting research for a school project, it is expected that they would come across, learn from, and discern from a wider array of materials than a 7-year-old on the internet playing video games. We suggest tailoring the definition of "child" to a user under the age of 13 to align with the federal Children's Online Privacy Protection Act (COPPA) standard. This would also allow for those over 13, who use the internet much differently than their younger peers, to continue to benefit from its resources.

[9] Caitlin Dewey, *California's New Child Privacy Law Could Become National Standard*, The Pew Charitable Trusts (Nov. 7, 2022), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/11/07/californias-new-child-privacy-law-could-become-national-standard.
[10] *Reno v. ACLU*, 521 U.S. 844 (1997).
[11] Jackie Snow, *Why age verification is so difficult for websites*, The Wall Street Journal (Feb. 27, 2022), https://www.wsj.com/articles/why-age-verification-is-difficult-for-websites-11645829728.
[12] *NetChoice v. Bonta* (N.D. Cal. 22-cv-08861).

5. The private right of action would result in the proliferation of frivolous lawsuits.

HF 1503 permits users to bring legal action against companies that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Minnesota's courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. As lawsuits prove extremely costly and time-intensive, it is foreseeable that these costs would be passed on to individual users and advertisers in Minnesota, disproportionately impacting smaller businesses and startups across the state.[13]

* * * * *

While we share the Committee's concern regarding the potential implications of automated systems and related technology, we encourage Committee members to resist advancing legislation that is not adequately tailored to this objective. We appreciate the Committee's consideration of these comments and stand ready to provide additional information as the Legislature considers proposals related to technology policy.

Sincerely,

Jordan Rodell
State Policy Manager
Computer & Communications Industry Association

[13] Trevor Wagener, *State Regulation of Content Moderation Would Create Enormous Legal Costs for Platforms*, Broadband Breakfast (Mar. 23, 2021), https://broadbandbreakfast.com/2021/03/trevor-wagener-state-regulation-of-contentmoderation-would-create-enormous-legal-costs-for-platforms.