March 14, 2024

House Committee on Judiciary Finance and Civil Law
Room 5, State Office Building
100 Dr. Martin Luther King Jr. Boulevard
St. Paul, MN 55155

RE: HF 4400, "Prohibiting Social Media Manipulation Act created, social media platforms regulated, and private right of action and attorney general enforcement provided" (Oppose)

Dear Chair Becker-Finn 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 4400 in advance of the House Committee on Commerce Finance and Policy hearing on March 4, 2024. CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] Proposed regulations on the interstate provision of digital services therefore can have a significant impact on CCIA members.

CCIA's members have been leading the effort to implement settings and tools to tailor an individual's online use to the content and services that are suited to their unique lived experience and preferences, including those for younger users.[2] For example, various services allow users to set time limits, provide enhanced privacy protections by default for known child users, and other tools to allow users to block specific sites entirely.[3]

CCIA appreciates the opportunity to detail several issues regarding the provisions included under HF 4400, including those related to potential conflicts with the First Amendment. We note that the comments that follow are not an exhaustive list as we are continuing to review the bill's language. We look forward to further discussions with the sponsor and lawmakers regarding the proposed legislation.

Foremost, CCIA has serious concerns regarding myriad ways in which HF 4400 conflicts with the First Amendment.

As further detailed throughout the following comments, provisions under HF 4400 raise constitutional concerns, specifically with regard to the First Amendment. The bill appears to

[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] Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children's Safety Online*, Disruptive Competition Project (Feb. 7, 2023), https://www.project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/.
[3] *See, e.g.*, Competitive Enterprise Institute, *Children Online Safety Tools*, https://cei.org/children-online-safety-tools/; CTIA-The Wireless Association, *Mobile Parent*, https://mobileparent.org/; Software & Information Industry Association (SIIA), *Keep Kids Safe and Connected*, https://www.keepkidssafeandconnected.com/.

compel the speech of covered social media platforms. The proposal also appears to restrict access to online information by users who would be subject to daily "engagement limits". Due to the vague definitions and broadly sweeping private right of action created under HF 4400, the measure is also likely to significantly chill speech as well. CCIA expands on several of these aspects in the comments below and stands ready to serve as a resource on this topic.

Algorithms are instrumental in providing better-tailored online experiences.

Several provisions under HF 4400 seek to alter the manner in which social media platforms narrow content that is shown to users. Banning personalization harms user experience and hinders access to relevant information, especially for children. It is also worth noting that the First Amendment prohibits the government from interfering with the right of private parties to exercise "editorial discretion in the selection and presentation"[4] of speech.

Currently, algorithmic feeds already serve content with increased relevance to individual users, prioritizing content that is more likely to be appropriate and of interest. By analyzing past interactions, browsing history, and other factors, algorithms contribute to curating a relevant and personalized experience. While algorithms personalize a user's experience, they can also help to introduce new topics and interests allowing users to discover creators, ideas, and communities they would not have found otherwise. And algorithms are able to do this efficiently — with vast amounts of content available, algorithms help users navigate information overload through prioritizing content and allowing users to find what they're looking for faster and with less effort.

Algorithms can also be used to encourage more positive experience online, including through the use of tools to identify and report illegal or dangerous content such as CSAM, copyright infringement, or content promoting terrorism in addition to helping guide users to helpful resources if they search for material related to self-harm, suicide, or depression.

HF 4400 includes several subjective terms tied to requirements for social media platforms.

HF 4400 includes several vague definitions that would make it impossible for covered social media platforms to come into compliance. For example, HF 4400 would require a covered platform to provide a mechanism for users to indicate whether a particular piece of content is of "high" or "low" quality and for an "algorithmic ranking system" to optimize content for a user that, among other provisions, "a varied set of account holders indicates is of high quality". HF 4400 does not specify what constitutes a "varied set of account holders" and, in fact, places the onus on the platform to explain what their understanding of the term is. Given the subjective nature of what an individual user deems as "high" or "low" quality and a lack of a uniform understanding of what a "varied set of account holders" encompasses, it is unclear what impacts this may have on overall user experience and renders it impossible to understand how these provisions feature in achieving the intended goal of the legislation. These provisions are also problematic when considering the bill's enforcement mechanisms as further detailed later in our comments.

[4] *Ark. Ed. Television Comm'n v. Forbes*, 523 U.S. 666, 673 (1998).

Similarly, HF 4400 defines "relevant forms of engagement with users" in such a vague way that it could arguably encompass the entirety of the social media platform as a service.

HF 4400's enforcement provisions are incredibly broad. The newly established private right of action would lead to a multitude of frivolous lawsuits.

HF 4400 allows a "person injured by a violation" to bring a civil action against a social media platform. However, the bill itself does not define what qualifies as an injury. Given the bill's subjective and vague terms, it is unclear whether a user could hold a covered social media platform liable for an algorithmic ranking system serving content that the individual user considers to be "low quality" especially given that the ultimate designation of whether a single piece of content is deemed "high" or "low" quality hinges on the ranking of a "varied set of account holders", which is also not adequately and clearly defined enough to provide any meaningful compliance roadmap.

By creating a new and broadly sweeping private right of action, HF 4400 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 businesses in Minnesota, disproportionately impacting smaller businesses and startups across the state.[5] Private rights of action generally risk shifting online services' resources to attorney's fees to defend against litigation rather than focusing on investments to enhance and improve users' online experiences. The constant threat of litigation faced by businesses of all sizes under HF 4400's vague terms would inevitably chill innovation.

Setting "engagement limits" on social media platforms is likely to have adverse impacts.

Setting arbitrary numerical limits and restrictions on existing networks are ineffective and likely to interfere with the developmental and engagement needs of individual users. Due to the way in which "relevant forms of engagement with users" is defined, this would arguably require shutting down certain services for users who have reached their daily engagement limit. Such limitations would limit user access to relevant and necessary information, impeding a user's ability to access open online information. This, again, raises concerns about whether HF 4400 would violate the First Amendment.

Many social media platforms are now used to convey and widely disseminate a variety of information, including alerts about public safety incidents and natural disasters. Social media platforms can also serve as a central meeting place for users to notify family and friends that they are safe during such occurrences.

[5] 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/.

HF 4400's provisions concerning default privacy settings are also vague and would encompass a broad array of services and contexts.

Under Subdivision 3, concerning "default privacy settings", HF 4400's provisions are extremely vague and likely to encompass many services. The sweeping nature of these provisions risks preventing a "network effect" from occurring entirely, which would also create a heavy barrier to entry for new online services and platforms, significantly degrade the user experience, and render platforms unusable.

For example, the bill would require a social media platform to prohibit, by default, a user's account or content from being discovered by anyone outside the user's network. While, on many platforms, a user may choose to restrict the sharing of their account information or content, it is not the default setting and this would also prevent users from reposting and sharing content by other users, which is a key feature and benefit of using social media platforms.

Similarly, the provision to prohibit certain interactions or other contact from an account holder that are not already within the user's existing extended network, unless the user initiates and welcomes the contact, raises questions about how users, for example, on platforms like LinkedIn, could reach out to new contacts and prospective employers/employees. This would conflict with the very purpose that the platform is intended to provide – career networking and recruiting. Further, the provision raises questions about how any "welcome" contact could be initiated and accepted if the contact is blocked by default for all users.

Subsection (b) presents a technologically infeasible requirement that would impose a disproportionate burden on device manufacturers. The provision would require a device operating system to, by default, "consider any device with parental controls enabled to have opted in to all the heightened protection requirements". Setting aside the fact that device manufacturers do not produce devices with state-specific settings, the requirement would also force manufacturers to continuously develop new ways to recognize opt-in signals, and new social media platforms appear constantly. This would be impossible to operationalize if the signal each platform uses differs as a device manufacturer would have to adhere to a diverse and constantly evolving set of opt-in mechanisms. Further, it is not clear whether this type of opt-in mechanism would be required at both the browser and device level, resulting in confusion surrounding when covered platforms are accessed via an application or a browser.

HF 4400's transparency requirements are extremely burdensome and could have harmful unintended consequences.

In 2021, a number of online businesses announced that they have been voluntarily participating in the Digital Trust & Safety Partnership (DTSP) to develop and implement best practices to ensure a safer and more trustworthy Internet, and have recently reported on the efforts to implement these commitments.[6] As digital services invest significant resources in

[6] Margaret Harding McGill, *Tech giants list principles for handling harmful content*, Axios (Feb. 18, 2021), https://www.axios.com/techgiants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html.

developing and carrying out trust and safety operations to protect users from harmful or dangerous content, they require flexibility in order to address new challenges as they emerge.

Many online platforms already voluntarily and regularly generate reports and make them publicly available on their websites. Since its launch, DTSP has quickly developed and executed initial assessments of how its member companies are implementing the DTSP Best Practices Framework, which provides a roadmap to meaningfully increase trust and safety online. This roadmap includes several commitments to transparency and content moderation disclosures, in addition to others, to which DTSP members are expected to adhere.[7]

The provisions under HF 4400 may be both overly prescriptive and counterproductive to the legislation's intended goals — rather than improving users' online experience, they might have the adverse unintended consequence of giving nefarious foreign agents, purveyors of harmful content, and other bad actors a playbook for circumventing digital services' policies. This is a critical reason why these algorithms are proprietary and carefully protected. Additionally, some of the required disclosures could be technically impossible or commercially impractical to implement, such as the requirement to disclose why a particular piece of content was promoted by the platform's algorithmic ranking system. Such a requirement could also violate protections under the First Amendment, by placing an undue burden on disseminating speech.

HF 4400 may also mandate the collection of additional user information that is not already being collected at a time when data minimization principles and additional privacy protections are being implemented across jurisdictions. Finally, the granularity and public nature of the reporting requirements could risk exposing sensitive business information.

* * * * *

We appreciate your consideration of our 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

[7] *See, e.g.*, DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* at 37 (July 2022), https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf (Appendix III: Links to Publicly Available Company Resources).