



April 25, 2023

House Judiciary 3 Committee
Room 421, Legislative Office Building
300 North Salisbury Street
Raleigh, NC 27603

RE: HB 644 - “Social Media Algorithmic Control in Information Technology Act.” (Oppose)

Dear Chair Blackwell and Members of the House Judiciary 3 Committee:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose HB 644. CCIA is an international, not-for-profit trade association¹ 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, HB 644 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

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

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>.

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 AI 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 for the integration of 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 Excellence⁸ is also leading federal regulatory efforts to establish practices for testing, evaluating, verifying, and validating AI systems. And, just this month, the Department of Commerce's National Telecommunications and Information Administration (NTIA) just announced a request for comments on AI accountability.⁹

The deliberate, thoughtful, and bipartisan fashion in which leaders at the federal level are approaching the wide variety of issues associated with artificial intelligence and algorithmic 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.

3. As drafted, HB 644 may actually put North Carolinians at greater risk of harm, including children that the bill seeks to protect.

CCIA is worried that businesses may be forced to collect personal information they don't want to collect and consumers don't want to give, and that data collection creates extra privacy and security risks for everyone. This forced 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

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).

⁹ NTIA Seeks Public Input to Boost AI Accountability (Apr. 11, 2023), <https://ntia.gov/press-release/2023/ntia-seeks-public-input-boost-ai-accountability>.

confirming that they are of age to be using these services. If North Carolina were to force companies to collect a higher volume of data on users even as others are requiring the collection of less data, it may place businesses in an untenable position of picking which state's law to comply with, and which to violate.¹⁰

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.¹¹ After 25 years, age authentication still remains a vexing technical and social challenge.¹² 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.

4. The bill lacks narrowly tailored definitions.

As currently written, the bill adopts the same definition of “operator” as used in the Children’s Online Privacy Protection Act (COPPA), but defines “minor” as anyone under 18. We suggest changing the definition of “minor” to a user under the age of 13 to align with the 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.

Due to the nuanced ways in which children under the age of 18 use the internet, it is imperative to appropriately tailor such treatments to respective age groups. 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. 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 definition of “algorithmic recommendation system” is also ambiguous. This current definition would potentially include a wide range of technology, capturing everything from spreadsheets to automated cameras. Further, it is unclear if terms such as “algorithmic recommendations” fit into the definition of an “algorithmic recommendation system” or if these are two different terms with two different meanings and compliance standards.

There is also confusion surrounding the “User Data Privacy” requirements in Section §75-71. The vague requirements not only undermine the success of personalization but also could create room for a more dangerous or harmful digital ecosystem. Social media platforms use algorithms to help prioritize content for the benefit of all users by enabling them to have personalized experiences. This technology has allowed for users, including teenagers, to follow and keep up to date with a tailored feed about topics they find interesting or relevant. Such algorithms are also useful in the context of user safety. Specifically, if a user, such as a teen, begins searching content around eating disorders or illicit drugs, they then can be directed to the relevant support communities or hotlines. Or, for example, through an algorithmically employed mechanism, users who search for terms related to suicide, self-harm, or depressive quotes can be redirected to mental health resources like the National Suicide Prevention Hotline.¹³ Many of these types of mechanisms would be difficult to implement or not feasible under HB 644.

¹⁰ 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>.

¹¹ *Reno v. ACLU*, 521 U.S. 844 (1997).

¹² 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>.

¹³ Annie Ta, *Introducing a more compassionate search experience for people in distress*, Pinterest Newsroom (July 22, 2019), <https://newsroom.pinterest.com/en/post/introducing-a-more-compassionate-search-experience-for-people-in-distress>.



5. Investing enforcement authority solely with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

HB 644 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 North Carolina'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 North Carolina, disproportionately impacting smaller businesses and startups across the state.¹⁴

Further, CCIA suggests providing at least a 30-day cure period to make sure digital services can consult with the attorney general and come into compliance before incurring penalties. This would allow for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. This would also focus the government's limited resources on enforcing the law's provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief but without the time and expense of bringing a formal suit. Businesses would also be better equipped with the time and resources to address potential changes rather than shifting focus to defending against litigation.

While we share the Committee's concern regarding the potential impact the internet may have on children, we encourage lawmakers to resist advancing legislation that is not adequately tailored to this objective. We appreciate your 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

¹⁴ 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-content-moderation-would-create-enormous-legal-costs-for-platform>.