



September 11, 2025

Massachusetts State House
Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity
24 Beacon Street
Boston, MA 02133

Re: S 51 – “An Act Relative to Social Media, Algorithm Accountability, and Transparency” (Oppose)

Dear Chairs Moore and Farley-Bouvier, Vice Chairs Payano and Hawkins, and Members of the Joint Committee on Advanced Information Technology, the Internet, and Cybersecurity:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully oppose S 51 in advance of the hearing on September 11, 2025.

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 and its members have a shared interest in protecting children and giving parents and adults simple but effective tools to provide a safe online environment for their families.

CCIA firmly believes that children are entitled to greater security and privacy online. Our members have designed and developed settings and 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 This is also why CCIA supports implementing digital citizenship curricula in schools, to not only educate children on proper social media use but also help teach parents how they can use existing mechanisms and tools to protect their children as they see fit.³ While CCIA shares the goal of increasing online safety, the bill fails to address our concerns:

Requirements under S 51 are not administrable or well defined, creating serious compliance questions for both businesses and users.

The bill’s definitions section begins with the phrase “unless the context clearly requires otherwise,” followed by definitions of the key terms. If the bill’s definitions can be altered based on a concept as vague as “context,” a covered entity cannot know in advance whether it is complying with the law or not. Such a provision is likely too vague to meet the Fourteenth Amendment’s Due Process Clause requirements.

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 Jordan Rodell, *Why Implementing Education is a Logical Starting Point for Children’s Safety Online*, Disruptive Competition Project (Feb. 7, 2023), <https://project-disco.org/privacy/020723-why-implementing-education-is-a-logical-starting-point-for-childrens-safety-online/>.



S 51 would require covered businesses to pay for burdensome and costly monthly algorithm risk audits by third-party auditors, “unless specified otherwise by the office.” Among other things, the audits will focus on the very vague “patterns of use that indicate or encourage addiction-like behaviors,” discussed in more detail below. Additionally, stakeholders identified as “experts in the mental health and public policy fields” — which notably lacks trust and safety practitioners — must annually “identify additional ways covered platforms cause harms to children” to enable regulations “based on the cumulation of the potential harms.” S 51 thus appears to presuppose that there will be “additional harms” each year, instead of considering that harms could be reduced and/or that there could be additional benefits.

The extensive compliance burdens also include detailed annual transparency reports, and “biannual reports” thereafter (which confusingly can mean twice a year or every two years). Leading digital services already voluntarily and regularly publish detailed transparency reports on their websites.⁴ The AG may fine an entity that “materially omits or misrepresents required information in a submitted report” up to \$500,000 per violation. Since it is not clear what qualifies as a violation, damages could easily be in the millions of dollars. In assessing the fine, S 51 instructs a court to consider whether the covered platform made a “reasonable, good faith attempt to comply,” which does not provide businesses with sufficient guidance to ensure they are in compliance.

S 51 risks forcing businesses to disclose proprietary information, undermining security.

As S 51 acknowledges, the designs, algorithms, and features that must be “made accessible to the public” under this bill may include information that is “trade secret, proprietary or privileged.” While the bill permits covered entities to request such information be “redacted from the copy of the report that is obtainable under the public records law and on the attorney general’s website” via a “confidential, in-camera review of requested redactions,” it is not clear if the office will grant the request, and malicious actors may nonetheless be able to make inferences regarding a company’s security practices even from partially redacted text. These disclosure requirements might unintentionally give nefarious foreign agents, purveyors of harmful content, and other bad actors a playbook for circumventing digital services’ safety mechanisms, making vulnerable users like children less safe.

CCIA recommends further limiting the information requested in the reports and the parties with whom it is shared. Doing so would allow businesses to be more candid, avoid overburdening regulators and businesses, and protect potentially sensitive information.

Terms such as “addiction” in this online context lack adequate scientific foundation.

Section 36(d)(ii) of the bill requires the algorithm risk audits to focus on “patterns of use that indicate or encourage addiction-like behaviors.” This concept lacks a concrete scientific meaning: humans engage in various compulsive and repetitive behaviors — some of which may

⁴ See, e.g., DTSP, *The Safe Assessments: An Inaugural Evaluation of Trust & Safety Best Practices* 37 (July 2022), https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf (Appendix III: Links to Publicly Available Company Resources).



negatively impact physical and/or mental health. These could range from binge eating unhealthy foods to exercising excessively to watching favorite shows for hours on end. However, these behaviors 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.’”⁵

The connected nature of social media has led some to allege that online services may be negatively impacting teenagers’ mental health. However, researchers explain that this theory is not well supported by existing evidence and repeats a ‘moral panic’ argument frequently associated with new technologies and modes of communication. Instead, social media effects are nuanced,⁶ individualized, reciprocal over time, and gender-specific.

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.⁷ 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.⁸ 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.”⁹

* * * * *

While we share concerns regarding the safety of young people online, we encourage you to resist advancing legislation that is not adequately tailored to this objective.

Sincerely,

Kyle J. Sepe
Regional State Policy Manager, Northeast
Computer & Communications Industry Association

⁵ Am. Psychiatric Ass’n, *Diagnostic and Statistical Manual of Mental Disorders: Fifth Edition Text Revision* (2022).

⁶ Amy Orben et al., Social Media’s Enduring Effect on Adolescent Life Satisfaction, PNAS (May 6, 2019), <https://www.pnas.org/doi/10.1073/pnas.1902058116>.

⁷ 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/>.

⁸ 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/>.

⁹ *NetChoice v. Yost*, 778 F. Supp. 3d 923, 955 (S.D. Ohio 2025).