January 15, 2026

New York Standing Senate Committee on Internet and Technology
Senate Hearing Room
250 Broadway, 19th Floor
New York, New York 10007

Re: Artificial Intelligence Hearing – "To discuss risks, solutions, and best practices with respect to the use of artificial intelligence…"

Dear Chair Gonzalez and Members of the Standing Senate Committee on Internet and Technology:

On behalf of the Computer & Communications Industry Association (CCIA), I write ahead of the New York State Senate's public hearing on the risks, solutions, and best practices associated with artificial intelligence. 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.

The Association has previously shared broader concerns with New York's AI regulatory efforts.[2] As a trade association whose members provide digital services across state and national borders, CCIA has a strong interest in ensuring that AI policy is risk-based and innovation-enabling. The Association's comments provide an overview of the importance of sensible governance in AI and raise concerns about Senate Bill S. 1169, the New York AI Act.

The RAISE Act Sets the State Down a Concerning Path

The recently enacted RAISE Act places obligations on developers of frontier models. The Association respectfully requests that the legislature work on improvements to the existing law addressing the concerns below, before considering additional AI legislation.

Among the RAISE Act's obligations is a requirement that they be held liable for the actions of third parties using their models. While such a provision is untenable in general due to the impossibility of predicting third-party uses, it is particularly problematic in the context of open source frontier models. If a car mechanic modified the engine of a driver's car in a way that caused it to explode, liability would lie on the mechanic, not on the engine maker. It is unclear why AI systems should be treated differently when third parties modify the model or the way in which it is used. Additionally, the third-party liability problem is exacerbated by the provision that states that entities cannot shift liability to users as a condition of use. This creates problems for both closed and open models—in either case, even if a user builds an unexpected application or uses the model in unexpected or unintended ways, the model developer would bear liability.

In short, the RAISE Act's misalignment reflects a broader approach by the state that is overly rigid, insufficiently risk-based, and disconnected from the realities of the AI ecosystem. As further

[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] CCIA, *CCIA Veto Request Letter on NY S 6953 (RAISE Act)* (June 13, 2025), https://ccianet.org/library/ccia-veto-request-letter-on-ny-s-6953-raise-act/.

discussed below, AI policy must instead be balanced, flexible, and grounded in a clear understanding of the distinct roles played by developers, deployers, and users.

AI Policy Must Be Balanced, Flexible, and Understand the Ecosystem

As AI evolves rapidly, it is crucial to find a balance in regulation to ensure the rules are not so rigid that they hinder innovation and U.S. competitiveness. Achieving this kind of balance requires thoughtful and adaptable legislation that is informed by the principles of responsible AI and can be applied across many different contexts. Rather than imposing overly detailed and narrowly tailored rules, the focus must be on establishing frameworks that enable the design of AI systems and allow them to serve society's best interests. Additionally, in the absence of a single federal framework regulating AI, any single state's efforts to implement broad regulation would likely place a state like New York at a competitive disadvantage by inhibiting the use of new technologies to further growth, while other states may not implement such obstacles.[3]

There are multiple entities involved in an AI system, including developers, deployers, users, hardware and software. It is crucial to correctly assign liability among them. Legislation should ensure that developers and deployers are not held liable for the harmful actions of users. Similarly, end-users should not be responsible for intentionally created flaws in an AI model, such as one that consistently produces biased outcomes. Correctly assigning responsibility ensures that liability falls on the party best positioned to prevent harm and be held accountable for any damages.

One example of this is two-factor authentication (2FA) and the transformation that password security has undergone in the last few years. If policymakers had adopted prescriptive regulations for privacy as it relates to 2FA, those rules would have quickly become outdated and potentially blocked secure innovations such as passkeys. The same risk applies to AI policy, especially prescriptive rules that lock in specific technical assumptions, licensing models, or training methods to a rapidly changing landscape.

Additionally, determining which practices constitute 'best practices,' both in AI governance and in technology policy more broadly, is not a matter of government preference, and it should not be dictated by prescriptive legislation. Meaningful best practices require consultation with the very practitioners who design, deploy and operationalize these systems, along with the relevant stakeholders who understand how AI functions in real-world settings.[4] As technologies like AI evolve, so do the safeguards, tools, and governance approaches that are most effective at navigating risk.

Existing Laws Already Address Many Aspects of AI

Despite the ongoing trend of AI-specific legislation, it is important to recognize that many of the risks commonly associated with AI are already addressed through existing federal and state frameworks. AI does not operate in a legal vacuum but rather, it is a tool used within regulated markets that are already governed by long-standing consumer protection, civil rights, privacy, and other product liability laws. Ahead of proposing such laws, it is crucial that policymakers consider what laws AI systems are already covered by. It is important to build upon existing legal protections

[3] CCIA, *Understanding AI: A Guide To Sensible Governance* (June 2023), https://ccianet.org/library/understanding-ai-guide-to-sensible-governance/.
[4] Digital Trust & Safety Partnership, *Best Practices for AI and Automation in Trust and Safety* (Sept. 2024), https://dtspartnership.org/best-practices-for-ai-and-automation-in-trust-and-safety/.

and focus narrowly on clearly defined gaps where demonstrable harms are not yet addressed. A balanced approach that does not layer expansive new liability regimes on AI developers will better protect consumers and preserve the innovation ecosystem.

The Importance of Digital Literacy and AI Education

In addition to thoughtful and targeted policymaking, CCIA believes that digital literacy and education are essential aspects of any effective AI governance strategy. Investing in digital literacy curricula for students, parents, and educators helps ensure individuals understand how AI systems work, their limitations, and how to engage with them critically and responsibly. This education empowers users to recognize when AI is being used, to question automated outputs, and to make informed decisions. CCIA encourages New York to explore the integration of digital literacy, as these efforts would complement existing consumer protection laws and equip individuals with the knowledge to navigate an increasingly digital world.

S. 1169 Carries Risks to Innovation and Compliance Burdens

S. 1169's broad definitions and requirements, including extensive external audits and opt-out mechanisms for any "high-risk" system, can create high compliance costs, especially for startups or researchers that do not have extensive legal systems or means. As CCIA has stated above, overly broad regulations can dampen innovation and divert crucial investment away from New York based on these requirements. If S. 1169's enforcement mechanisms are used to expose developers to liability for algorithmic discrimination and concerns even when outcomes are driven by third parties, this could disincentivize participation in the New York tech ecosystem. CCIA's previous veto letter on the RAISE Act highlights similar concerns about liability regimes that misunderstand where liability should lie within the AI ecosystem.[5]

Additionally, state AI laws can overlap with existing federal and sectoral rules, which is likely to cause confusion without clear preemption or coordination strategies. The Association warns about inconsistent standards that would increase operational complexity.

We appreciate your consideration of these comments and stand ready to provide additional information as the state considers proposals related to artificial intelligence and technology policy.

Respectfully submitted,

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

[5] CCIA Veto Request Letter on NY S 6953 (RAISE Act), *supra* note 2.