January 15 2026
Written Testimony on Regulation of High-risk use of AI in the Private Sector
Submitted by: Hasan Khan and Shruthi Velidi (DSA Tech Action Organizing Committee)

Harm in plain sight: Redefining existential AI risks

Recent legislation in New York (See: RAISE Act) has focused on mitigating discrete catastrophic outcomes of large AI systems (applicable only to systems that have a compute cost of over $100M) where more than 100 people die or $1B amount of financial damage occurs. While such crisis scenarios caused by AI must be regulated, broader and more substantive controls on AI systems of all sizes need to be introduced across the private sector. This framing of "high risk" use cases of artificial intelligence excludes real and ubiquitous harms (that disproportionately impact marginalized and working class New Yorkers), currently being perpetrated by AI use.

Defining "high risk AI"
We argue that a definition for "high risk" AI should focus on the intended use and audience rather than the algorithm complexity or compute cost of the system. We support SB1169A's approach of aligning risk with impact on consequential decisions and the bill's clarity on the scope of what constitutes a substantial factor in a consequential decision. (See SB1169A, Section 85.4,13). It should be noted that we also support SB1169A's inclusion of systems that have a "material impact on the statutory or constitutional rights, civil liberties, safety, or welfare of an individual in the state" as high-risk.

In addition, we recommend that any assessment of risk should also include an evaluation of an organization's ability to measure and mitigate potential harms that may arise with the deployment of this AI system. Evaluations can include, but are not limited, to the degree to which outcomes and decisions of a system can be easily explained, the degree of human oversight and control to challenge and remove harmful content (both by the end user and the developer/deployer), the ability of end-users to receive redress in the case of unfair outcomes, the layers of protection in place to protect sensitive data, the visibility into the inputs of the AI system and its data provenance, etc. Under the definition put forth by SB1169A, a corporation can easily choose to not classify its social media platform as "high risk", However, if we broaden the scope of high-risk, we make it harder for corporations to find loopholes to avoid risk management obligations.

Prohibited uses of AI
While an exhaustive list of prohibitive use cases is hard to develop and maintain by the State (given the rapid rate of AI development and deployment), we argue that certain uses of AI should be foundationally prohibited, regardless of the degree of impact on consequential decisions and civil liberties. We support SB1169A's inclusion of "social scoring AI systems" as prohibited (See SB1169A, Section 89-a). We also recommend expanding this prohibited list to include the use of AI to develop and distribute nonconsensual, sexual images or deepfakes (see recent case of Grok's image generator tool).