Valerie S. Mason
Chair

Ian McKnight
District Manager

505 Park Avenue, Suite 620
New York, N.Y. 10022-1106
(212) 758-4340
(212) 758-4616 (Fax)
www.cb8m.com – Website
info@cb8m.com – E-Mail

The City of New York
Community Board 8 Manhattan
Social Justice Committee
Monday, March 23, 2026 - 6:30 PM
This meeting was be conducted via Zoom

Minutes:

Committee Members Present: Sarah Chu, Saundrea I. Coleman, and Wendy Machever*

**Public Member*

Approximate Number of Public Attendees: 8

1. Alex Bores, Assemblymember for the 73rd District of New York, to discuss the Responsibility AI Safety and Education (RAISE) Act - Bill A6453A

a. Assembly Member Alex Bores sponsored and led the passage of the NY RAISE Act. He provided background on the RAISE Act and its scope:
   i. AI intersects with social justice in many ways, but the RAISE Act was intentionally focused on the most extreme, catastrophic risks from AI development. Bias and discrimination, labor force impacts, and child safety are also serious risks, they are not covered by this bill.
   ii. The bill targets risks that cannot be remediated after the fact: bioweapons development enabled by AI; AI systems operating outside of human control; and AI being used by bad actors to repress populations.
   iii. The core philosophy is that because these harms cannot be undone, responsibility for testing and eliminating them must rest with the companies themselves before deployment.

b. The original version of the RAISE Act contained four provisions:
   i. Safety plan: Developers must maintain and publicly disclose a safety plan and must amend it before — not after — changing their practices.
   ii. Critical safety incident reporting: Developers must notify the state government of defined critical safety incidents as they occur.
   iii. No-release requirement: Developers may not release a model that fails their own internal safety tests — drawing on the tobacco and fossil fuel industry analogy, where companies knew of harms but continued releasing products.
   iv. Third-party audit: An independent (non-governmental) auditor would verify that companies are following their stated safety plans, analogous to financial accounting audits or SOC 2 security audits.

c. Assembly Member Bores described the bill's development and the lobbying campaign mounted against it:
    i. August 2024: Initial draft circulated to major AI developers for feedback; responses were substantive and largely in good faith.
    ii. December 2024: Revised draft; additional feedback received.
    iii. March 2025: Bill formally introduced.
    iv. May 2025: Bill first passed committee; amendments made. At this point, engagement escalated from regional to national lobbyists. National lobbyists appeared to operate under a directive to: (1) block any frontier safety bill anywhere; (2) confine such legislation to the federal level; and (3) if it must happen at the state level, limit it to California.
    v. June 2025: Further amendments; bill passed the legislature on the final day of the Senate session in overwhelming bipartisan fashion — a majority of Assembly Republicans voted for it and every Senate Republican voted for it.
d. Despite A6453A being a state-level bill, there were aggressive industry tactics during this period, including text message campaigns targeting constituents in the 73rd District from AI companies and the involvement of global CEOs and major companies.
e. After negotiations with the Governor and further industry pressure, the final enacted version of the RAISE Act retained the first two original provisions and added a new enforcement mechanism:
    i. Safety plan requirement (enacted): The largest AI developers — currently Meta, Google, xAI, OpenAI, and Anthropic — must publicly disclose detailed safety plans and adhere to them.
    ii. Critical safety incident reporting (enacted): Covered companies must disclose critical safety incidents to New York State government.
    iii. Establishment of Office of AI Safety (new): A state office dedicated to AI safety is established, funded by assessments on covered companies, with the following authorities: to issue rules and regulations for expanded reporting; monitor AI development as it occurs; and provide annual recommendations to the legislature on further improvements needed.
    iv. The third-party audit provision and the no-release-on-failed-tests provision were not included in the final enacted law.
    v. A subsequent clean-up bill passed the legislature approximately two weeks before this meeting, resulting in what Assembly Member Bores described as objectively the strongest AI safety law in the country.
f. Assembly Member Bores offered observations applicable to future AI-related legislation:
    i. Industry framing: Many companies treat AI regulation as a winner-take-all race and catastrophize even light-touch provisions. One company's own lobbyist acknowledged that the original, stronger version of the RAISE Act would have required approximately one full-time employee to comply.
    ii. The "you don't understand" deflection: Companies often argue that AI is too complex for non-experts to regulate. Assembly Member Bores noted his master's degree in computer science and a decade of industry

experience, but emphasized that the impacts of AI on human beings are not inherently technical and do not require technical expertise to address — values-based accountability is both legitimate and sufficient.

iii. Centering human impact: Legislators and advocates should lead with the real-world effects on everyday people and not be deterred by complexity arguments.

g. Q&A and Discussion (summarized for brevity)

Q: Now that AI-generated music can be in the style of or attributed to artists — including deceased artists — without their consent, what legal challenges are anticipated?

AM Bores responded that there are two distinct issues:

- Transparency and disclosure: The public should know when content is AI-generated. Disclosure does not make AI-generated art inherently bad — there are legitimate creative uses — but informed consent requires knowing what one is engaging with.
- Training data and fair use: The question of what was used to train AI models and how to treat the underlying artwork is currently being litigated. Assembly Member Bores's policy position (not legal opinion) is that use of AI to replicate a specific artist's style raises genuine fair use challenges and should not be permitted. These questions remain unsettled across multiple active court cases.
- Courts have largely held that works generated by AI cannot be copyrighted, as they are the product of a statistical process rather than human authorship. Original artists who hold distribution rights can still profit from their work. Some emerging business models (e.g., Timbaland's reported project) involve licensing all underlying training data from individual artists.

Q: Several interrelated concerns were raised about the following:

- AI systems as utilities: Suggested that because AI is becoming infrastructure-level in its penetration, utility-style regulation is appropriate.
- Factual inaccuracy ("hallucination")
- Self-harm and mental health: Referenced reports of AI systems providing harmful responses to vulnerable users.
- Energy consumption: Noted a personal electricity bill increase attributed to AI data center demand, and concern about projected water consumption by AI infrastructure. Acknowledged the tension with New York State's interest in attracting semiconductor manufacturing and data center jobs, particularly upstate.

AM Bores responded that he published a comprehensive AI framework approximately one month prior to this meeting, covering eight topic areas and 43 sub-points addressing the full range of AI governance questions — including accuracy, safety, and energy. (See attached) Key themes include:

- Surveys show roughly 10% of Americans want no AI development at all; 10% want no regulation whatsoever; and 80% see both upside and downside and want reasonable guardrails.
- Support for "AI that works for us": AI that helps doctors diagnose disease — not helps insurers deny claims; AI that helps clean the ocean — not pollutes the internet; AI that

provides accurate information quickly — not spreads disinformation; AI that helps people live — not tells people how to live.
- Democratic accountability: The American people, not Silicon Valley billionaires, should determine how AI develops.
- Speed of change: AI governance cannot move at typical legislative timelines. The urgency is real.

Q: Why have more states not introduced similar legislation?

AM Bores is working with a nine-legislator group spanning seven states on AI safety work. Last year, activity was concentrated in blue states. This year, red states including Utah, Nebraska, and Oklahoma have active bills; Oklahoma's may pass this session. AI safety legislation has structural advantages over privacy legislation — because models are trained only once, a safety law in one or a few states effectively protects the rest of the country. This makes it somewhat less critical that every state act individually, though continued action is encouraged.

Q: Will the Office of AI Safety created by the RAISE Act have authority to address other AI harms such as bias, discrimination, labor force impacts, and child safety?

AM Bores stated that the Office's rulemaking authority is confined to the original scope of the RAISE Act. Addressing broader harms will require additional legislation, which he and colleagues are actively developing.

Q: AI is being used in law enforcement contexts and is there anything analogous to a lie detector test to assess AI honesty?

AM Bores responded that AI labs conduct internal testing on honesty metrics, and independent third parties also conduct evaluations. He noted interesting current research on how training choices affect model honesty — for example, models trained to treat certain shortcuts as acceptable may generalize that permissive attitude to other domains, while models not given that permission may develop and exhibit a broader pattern of deceptive behavior. He described this area as active and evolving.

2. **Old Business**
3. **New Business**

This meeting ended at approximately 7:06 pm.

Sarah Chu, and Saundrea I. Coleman, Co-Chairs

ALEX BORES' AI POLICY FRAMEWORK

Giving Americans Power, Protection, and a Stake in the AI Economy

1. PROTECT KIDS AND STUDENTS

Parents deserve to know when their children are interacting with AI, and kids deserve protection from exploitation. Smart rules can protect children while preserving AI's educational benefits.

- **Give parents visibility into their children's AI interactions**
- **Require age verification and parental consent for AI tools** that present serious risks to minors, including chatbots designed to elicit a romantic connection
- **Require all chatbots intended for repeated interactions to screen for messages** indicative of potential self harm and refer users to mental health resources
- **Prepare our kids for the jobs of the future** by teaching them about AI and how to use it
- **Encourage schools to set clear guidelines for when AI should be used and when it should not,** and update assignments to ensure they are effectively teaching the skills we intend (e.g. without guardrails, assigning an at-home essay no longer teaches writing or critical thinking)
- **Explore where AI can benefit education,** such as personalized tutoring (with monitoring by both teachers and parents)
- **Ban AI-generated child sexual abuse material,** with criminal penalties for creation and distribution, and legal liability shields for effective red teaming.

2. TAKE BACK CONTROL OF YOUR DATA

In the age of AI, your personal data is more valuable than ever. You should control who profits from it.

- **Pass a national data privacy law** giving all Americans the protections that currently only exist in some states
- **Establish clear data ownership standards**—your data, by default, belongs to you
- **Prohibit companies from selling your personal data** without explicit consent
- **Require clear disclosure when you're interacting with AI** instead of a human
- **Give consumers the right to know what data AI systems have collected about them**
- **Give consumers the right to know what kinds of data AI models trained on**

3. STOP DEEPFAKES

When you can't trust your own eyes and ears, democracy itself is at risk. But deepfakes are actually an easily solvable problem with the right policies. We need technical standards and legal consequences to restore truth to our informational ecosystem.

- **Encourage the use of free, open source metadata standards** (e.g. C2PA) that prove whether a piece of content is real or AI-generated
- **Enable users to trace the origin and editing history of images, video, and audio** through the same standards
- **Create penalties for malicious deepfake creation and distribution** in sensitive domains like revenge porn, political campaigns, or scams

4. MAKE DATA CENTER INVESTMENTS WORK FOR PEOPLE

AI companies shouldn't stick working families with the bill while reaping billions in profits. Our electric grid needs upgrades, but government has not found the resources to pay for them other than sticking ratepayers with higher bills. Now, we have an industry with nearly unlimited capital that wants to build data centers, and is willing to invest in modernizing our grid as a part of that. We need policies that ensure those investments go to green energy and to grid upgrades instead of to expanding the use of fossil fuels.

- **No utility rate hikes** for residents to subsidize data center energy costs
- **Hold data center developers accountable** through binding community benefit agreements
- **Expedite data centers that use new green energy and cover 100% of the costs of grid upgrades,** while delaying or cancelling data centers primarily powered by fossil fuels
- **Leverage private capital for data centers to repair our electrical grid** and accelerate clean energy
- **Monitoring water usage of large data centers** to ensure there is no detrimental impact to local communities
- **Close loopholes that let data centers dodge property taxes**

5. PROTECT AND SUPPORT WORKERS

AI is changing the nature of work. The question is whether workers are left behind or given the tools to thrive. Alex believes technology should empower workers, that's how we build the right kind of future.

- **Require large companies to report AI-related workforce changes**
- **Create tax incentives for businesses that invest in upskilling existing employees**
- **Invest in community colleges and job retraining programs**
- **Ensure AI cannot be the sole decision-maker** in hiring, firing, or promotion decisions
- **For jobs that currently require a license or permit for a human to do, require the same of AI for a transitional period,** to ensure workers who have invested substantial sums in attaining the right to do a job are not wiped out
- **Tax large AI companies and return the gains to Americans** through an AI dividend, to ensure every American benefits from AI-driven productivity and that the American people get a share of the profits from a technology they helped build – not just AI labs.

6. NATIONALIZE THE RAISE ACT: ESTABLISH SAFETY STANDARDS FOR FRONTIER AI

We don't let pharmaceutical companies sell drugs without FDA approval. We shouldn't let tech companies deploy potentially dangerous AI systems without safety testing.

- **Require independent safety testing** for the most powerful AI models
- **Mandate reporting of cybersecurity incidents** involving AI systems
- **Restrict government use of AI tools** from foreign adversaries like China, with appropriate exceptions for security research
- **Create accountability mechanisms for AI systems** that cause demonstrable harm
- **Engage in diplomacy to lower the temperature on an AI race;** even during the height of the Cold War, we had the red phone to Moscow

7. BUILD GOVERNMENT CAPACITY TO OVERSEE AI

Democracy requires a government that actually understands the technology shaping our society. Right now, AI leaders know far more about what's coming than the regulators trying to keep up. That has to change.

- **Fund the Center for AI Standards and Innovation (CAISI) within NIST**
- **Expand technical expertise across the federal government** through special hiring authorities, fellowships, and advisory boards
- **Require large AI developers to provide confidential disclosures to regulators** about training scale, compute use, and capabilities
- **Develop contingency plans to handle rapid AI improvements** and large-scale risks before they become crises

8. KEEP AMERICA COMPETITIVE

The AI race isn't just about economic competitiveness—it's about ensuring democratic values shape this technology's future. America can win this race while protecting workers, consumers, and communities. We don't have to choose between innovation and safety.

- **Federal funding for AI research at universities and national labs,** including research on AI alignment—ensuring these systems reliably do what we tell them to
- **Support for American AI companies developing safe, beneficial applications**
- **Reasonable regulation that protects people** without strangling innovation
- **Work with allies to establish verifiable international AI safety standards,** including around military applications
- **Strategic export controls to maintain America's AI lead over adversaries**
- **Keep the door open to negotiated international limits** that reduce dangerous AI arms-race dynamics