



New York City Council Technology Committee
October 28, 2024
Oversight Hearing: The Use of Automated Decision Systems
and Artificial Intelligence
by New York City Agencies

Testimony by:
Cynthia Conti-Cook
Director of Research and Policy
Surveillance Resistance Lab

Written submission uploaded and sent by email on October 31, 2024

Thank you to Chair Gutiérrez, and members of the committee, for holding this public hearing and allowing us the opportunity to share our deep concerns about how this administration has continued prior administrations' opacity around the harmful uses of machine learning and other automated systems that some New York City agencies have been using for more than a decade.¹

The Surveillance Resistance Lab investigates how the expansion of corporate technology solutions in government (data collection, AI, chatbots, etc.) can undermine democratic engagement and civic space, as well as cause real harm to communities reliant on government services and on accurate information from government communications. These harms are in addition to the more commonly cataloged privacy harms created by technology.

Our testimony emphasizes two points. First, we call for urgent legislative intervention, including amending Local Law 35 to mandate more consistent reporting across agencies with consequences for city vendors that refuse to comply with Local Law 35's reporting requirements, including describing training data. We highlight specific aspects of the Office of Technology and Innovation's (OTI) testimony by representative Alex Ford regarding the MyCity chatbot to illustrate this need.

Second, we urge that the bills in question at this hearing be revisited given the obvious need for more robust intervention and regulation of machine learning (or "AI") and automated systems. While we are generally aligned with the intent, in order to meet the stated goals and protect the public from corporate capture and aggressive marketing strategies of "AI" vendors, these bills must include mandates for agencies to demonstrate that they have engaged the impacted communities and advocates for those communities around the problems the agency seeks to solve, and has done its due diligence in assessing how to prioritize those problems based on the agency's limited resources.

If the agency has demonstrated that a prioritized problem could best be solved through an expensive long-term tech solution, they must also use a procurement process that enhances government and public transparency, accountability, and oversight over foreseeable harms and long-term financial and other costs, potential municipal liability, and the impact of the technology on the communities it may be used in, along with clear consequences for vendors that fail to comply with these requirements.

This is particularly important when those machine learning ("AI") systems are incorporated through software updates the agencies already have without proper public

¹ <https://ainowinstitute.org/publication/confronting-black-boxes-a-shadow-report-of-the-new-york-city-automated>

sector vetting. These mandates must be legislated given the obviously reckless and rampant adoption of consequential technologies across the City. It should be the public, and not the vendors, that are served by the power of the public purse, and the public's interest should be what defines how technology should be used.

Amend Local Law 35

First, we call for urgent legislative intervention, including amending Local Law 35 to mandate more consistent reporting across agencies and clear consequences for city vendors that refuse to comply. Government mandated reporting should dictate what information the vendor expects to disclose, such as training data, rather than letting the vendor's contract language trump public policy.

The OTI testimony about the MyCity chatbot illustrates how backwards the relationship between the NYC public sector and its corporate vendors is. It should be the government on behalf of the public interest who decides when government reporting, such as that mandated by Local Law 35, should inform the contract terms and trump any conflicting pre-existing terms.

The harm of a vendor's refusal to comply with mandatory reporting requirements was showcased in the multiple documented failures of the MyCity chatbot in its first year. The chatbot made recommendations that, if followed, would have resulted in unlawful discrimination, theft, and other abuses by landlords, employers, and small business owners and led to serious harm to vulnerable New Yorkers.² The OTI's testimony in response to questioning about the source of these failures suggested that these were merely a matter of grammatically incorrect sentences.

In contrast, news headlines such as "NYC's AI Chatbot Tells Businesses to Break the Law," highlights the seriousness of the potential harm. Beyond the probable but still speculative harms that this broken bot caused is the undeniable irreparable harm to public trust in government communications about legal information—trust that is difficult to rebuild once broken.

Councilmember Erik Bottcher asked the obvious question about how such a monumental failure could occur, inquiring about what information, or training data, was fed into the chatbot such that it produced such wildly wrong answers.³ The government's reply was as informative as disappointing—that the contract obligations

² <https://themarkup.org/news/2024/03/29/nycs-ai-chatbot-tells-businesses-to-break-the-law>

³ Minutes 54:00-59:00

with the vendor prevented it from disclosing that information. What the government meant to say was that the vendor claimed that the training data it used to generate the chatbot was “proprietary” and therefore would not disclose the information—as documented in the 2023 algorithmic compliance report.⁴

In addition to deferring to the vendor’s refusal to comply with mandatory reporting, government testimony about the chatbot revealed yet another example of how the tail is wagging the dog: when Bottcher asked how the government tested the chatbot, OTI testified that it was the “business owner” who decides whether the chatbot is effective, deflecting responsibility for this epic failure from OTI, even though it is the agency that procured the chatbot.⁵

This comment revealed how the government has completely abdicated its responsibility to hold its vendors to high standards when serving the public. The MyCity chatbot has been called out by the public, the media, multiple advocates at the September 30 hearing on MyCity, and many advocates at this hearing who all agree that this chatbot is not effective, dangerous, creates potential liability for the city due to the foreseeable harms it invites, plus it has dramatically undermined public confidence in government communication, while withholding necessary information that would explain how this went sideways.

Harm to public trust in government communication has been chronically underplayed by AI risk frameworks globally, circumventing the stricter scrutiny that these systems deserve from the public, government legal departments, and in all design, development, and deployment decisions. The potential for the City’s rapid adoption of technologies, including those that incorporate AI, calls for mechanisms for enforcing consistent reporting and consequences for companies that refuse to play according to public sector rules.

We cannot continue to allow the government to defer to the vendor regarding when its contract and trade secrets trump government mandatory reporting. The corporate culture around secrecy and proprietary relationship to its intellectual property is at odds with the public’s interest in transparency, adversarial testing, and accountability. This impossibly perplexing backwards power dynamic with the vendor is exactly the kind of result that governments can expect when they have been subjected to corporate “too big to lose your contract” lock-in.

⁴ <https://www.nyc.gov/assets/oti/downloads/pdf/reports/2023-algorithmic-tools-reporting-updated.pdf> (42-43)

⁵ Exchange at minutes 54:00-59:00

Our March 2024 report on MyCity quotes Professor Keith Breckenridge to define corporate lock-in:

in the context of the information economy as the “familiar, almost banal” corporate ambition to dominate “bounded networks of compatible resources and fiercely defended terrains of control over the global market in personal communications.” We all experience this as Apple or Google customers whose options for headphones, chargers, software, and other services are determined by which devices we own. Companies have also recognized centralization of city data as an opportunity to lockin their products as “proprietary architectures”—durable infrastructure that guarantees a long-term dependency by the state on companies. This “lockin” between companies and the state mirrors that of customers locked in, for example, to Apple or Google.

Corporate lock-in explains OTI’s frustrating testimony not only in regards to the failure to comply with Local Law 35, but regarding when OTI believes a product, like the “chatbot” is “effective” and ready for deployment—OTI testified that whether the chatbot was effective is decided by the business owner, not the government.⁶ This is backwards—contrary to OTI’s testimony, it should be the government on behalf of the public interest who decides when a product satisfies the public’s needs.

For this reason, in addition to mechanisms to enforce reporting compliance under Local Law 35, we also need strong measures to protect the public interest from corporate lock-in through opaque and anti-democratic procurement processes.

Revisit the bills 0199, 0926, and 1024 to require democratic protections and technology procurement that protects public access to information, transparency, accountability and oversight

The OTI testimony at this hearing made clear that New Yorkers should already be concerned that corporate vendors, their contract lawyers, and their marketing teams are setting the pace for public sector AI policy and are impacting all other policies as a result. Like public policies, these technologies have potentially serious life-changing consequences for the New Yorkers subjected to them. Unlike public policies, however, it is harder to determine when someone has been subjected to decisions made by a machine learning or automated system and even harder to hold governments

⁶ Minutes 54:00-59:00

accountable for those decisions when they are discriminatory, inaccurate, extractive, or otherwise abusive of power.

To unravel the programming that resulted in such a decision, to prevent similar future mistakes by the system, and to maintain community control over how these systems are deployed, New Yorkers need robust protections for access to information, opportunities to dissent, access to courts, and extensions of these democratic tools through the government to the vendor. Communities must be able to rely on their ability to leverage the government to protect them from technology companies incentivized to gather their data, profit off their profiles, and manage their behaviors towards commercial activities.

To enact the intentions of the bills in question at this hearing, agencies must be required and resourced to perform their administrative due diligence in engaging the public around the problems the agency needs to solve on behalf of the public and how to prioritize those problems. Agencies cannot abdicate their responsibility to informed public engagement by circumventing administrative procedures and hiding behind opaque procurement processes and vendor's insistence on contract terms.

These bills must include mandates to agencies to demonstrate that they have engaged the impacted communities and advocates for those communities around the problems the agency seeks to solve, and has done its due diligence in assessing how to prioritize those problems based on the agency's limited resources. This includes protections for the resources they need to maintain deep relationships with city communities through unionized agency staff that hold deep expertise and can leverage union power to protect the future of their work and their agencies' constituencies from harmful technology.

If the agency has demonstrated that a prioritized problem could best be solved through a tech solution, they must also use a procurement processes that enhances government and public transparency, accountability, and oversight over foreseeable harms, potential municipal liability, and the impact of the technology on the communities it may be used in, along with clear consequences for vendors that fail to comply with these requirements.

In previous testimony, we have shared concerns about current procurement processes that allow tech corporations to increase their hold on city digital infrastructure with minimal transparency, process, or oversight. As described above, this kind of corporate lock-in gives corporate vendors dominant power to dictate the terms of its public sector policies and services, illustrated by the vendor's refusal to comply with mandatory reporting for the broken MyCity chatbot.

Another key illustration of this dominant power is the Master Service Agreement contract. If the Council members had asked OTI questions about the cost of the chatbot, or whether the costs would be adjusted or refunded given how ineffective and harmful it proved to be, it would have been nearly impossible to fact-check OTI's answer, if they could answer at all. For a decade, big technology corporations have enjoyed the opacity and complexity of Master Service Agreements that hide the cost of their services and make it nearly impossible to calculate for members of the public—even when we have obtained copies of their mammoth contract.⁷

Along with pilot or demonstration project procurement, Master Service Agreements are anti-democratic, invite non-competitive procurement and pave the way for more sole-source vendors to take advantage of the city, and make the public vulnerable to exactly the kind of asymmetrical power dynamic that results in expensive and failed products like the MyCity chatbot with no accountability for the vendor. This is just one example of how corporate lock-in prevents community control over local governance—and it is the tip of the iceberg.

For example, the government testified during the hearing that agencies procuring AI “still need to do all the things they would need to do for procuring technology” and that there were multiple points of review, oversight, privacy, cybersecurity, and other safety compliance that happen during the procurement process. The government confirmed that these robust processes are why we should trust that all technology used by the government, including “AI”, has been vetted according to high standards.⁸ However, what OTI failed to mention was that more technology, including machine learning (“AI”), is being used by agencies without going through the full procurement process. In fact, this administration itself has advocated for expanding agencies’ options for using machine learning and other automated technology without going through the robust procurement processes in order to enhance “innovation”.⁹

Regarding demonstration project procurement and the Procurement Policy Board's recent expansion of the rules governing why and how long agencies can use it to pilot a technology, we reference our prior testimony for the September 30 MyCity hearing about the importance of preventing pilot or demonstration project procurement from

⁷ https://surveillanceresistancelab.org/wp-content/uploads/MyCityINC_March2024.pdf

⁸ At 39:00-40:00

⁹ <https://www.crainsnewyork.com/politics-policy/adams-administration-changes-procurement-rules-encourage-ideas>

becoming the exception that swallowed the rule.¹⁰ Allowing more agencies to engage with tech companies without going through a public request for proposal (“RFP”), competitive bidding, contract compliance, transparency, cybersecurity, privacy, and oversight processes leaves New Yorkers vulnerable to tech companies. Allowing them to do so for longer periods of time and without any intention to open up the process for competitive bidding is antithetical to innovation. We refer the Committee to our in-depth August 2024 testimony to the Procurement Policy Board opposing the expansion of demonstration project rules.¹¹

Conclusion

For that reason, while we agree with the goals of the Committee on Technology in creating more oversight of the city’s use of machine learning and automated decision-making systems, we would invite a deeper conversation about including strong intervention points, transparency, and accountability in the technology procurement process, starting by limiting the use of demonstration project procurement and by amending Local Law 35 as described above to better fulfill its mandate.

¹⁰ <https://surveillanceresistancelab.org/wp-content/uploads/Lab-MyCity-Testimony-Sept-30-2024.pdf>

¹¹ <https://surveillanceresistancelab.org/wp-content/uploads/Lab-Testimony-Challenge-Based-Reform-Aug-2024.pdf>