

TESTIMONY OF:

Jacqueline Gosdigian, Supervising Policy Counsel

BROOKLYN DEFENDER SERVICES

Presented before

The New York City Council Committee of the Whole

Oversight Hearing Examining the Risks Posed by Artificial Intelligence

October 5, 2026

My name is Jacqueline Gosdigian. I am a Supervising Policy Counsel at Brooklyn Defender Services (BDS). BDS is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. I would like to thank Speaker Menin for convening this critical hearing examining the risks posed by artificial intelligence (AI).

For 30 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality. After 29 years of serving Brooklyn, we expanded our criminal defense services to Queens. We represent over 40,000 people each year who are accused of a crime, facing the removal of their children, or facing deportation. Our staff consists of attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS also provides a wide range of additional services for our clients, including civil legal advocacy, assistance with the educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

BDS' Seizure and Surveillance Defense Project (SSDP) engages in direct representation, impact litigation, and legislative advocacy to understand and address the ways property seizure and surveillance practices impact arrests, prosecution, and policing of the communities we serve. SSDP researches surveillance technologies and tracks patterns of NYPD surveillance used across New York City to understand and challenge the NYPD's billion-dollar surveillance apparatus. Through this work, we have become experts in the technology—including Artificial Intelligence—that is used to justify and conduct the surveillance, targeting, policing, and arrest of Black, brown, and immigrant New Yorkers.

Many of the people that we serve live in heavily policed and highly surveilled communities. As a result of heightened-policing and surveillance, the people we represent are often the test subjects

of experimental and error prone artificial intelligence software that is being rapidly acquired by city agencies including the NYPD and DOC. These communities are also predominantly low-income communities of color, who are subject to automated decision systems and artificial intelligence (AI) in the most important areas of life—public housing and benefits, the public transit system, and throughout our policing systems.

Private AI Companies Rely on the Public for Data to Train their Systems

Artificial intelligence refers to a broad range of computer-based and data-information systems and tools that have the ability to digest large amounts of information, make decisions based on predictive modeling, process data to solve problems, and perceive and recognize content and images, without being directly prompted by computer code.¹ To “train” or “teach” an AI or automated decision making system, software developers must input large amounts of data into these systems. When city agencies acquire third-party AI software, the data uploaded by the city is then used by developers to train and grow their AI tools. The data New Yorkers share with the city is often highly sensitive and private—as they apply for city services, public benefits, and seek support. Beyond this, the city has vast surveillance systems that follow New Yorker’s movements without their knowledge—from CCTV cameras and license plate readers, to the OMNY system. When uploaded to AI enabled technology programs, this massive collection of highly sensitive data is used by developers to benefit the growth of their systems at the risk to privacy and liberty of New Yorkers.

As the Council considers ways to address the risks posed by AI, we encourage you to consider the multitude of ways the rights to New Yorkers’ data and privacy have been eroded and to question the decisions made by AI systems in city agencies. As we explain below, the AI systems used by the city are disproportionately trained on the data extracted from the most surveilled communities—low-income communities of color. We urge the Council to consider the inequities of the data surveillance economy and how this biased information further reproduces and entrenches the racial biases endemic to these institutions.

Unchecked AI Is Being Used Against New Yorkers Already, Beyond the Reach of the Courts

As public defenders in Brooklyn and Queens, we see AI and machine learning systems used daily in criminal investigations, in justifying family separation, and against people seeking unemployment benefits, facing evictions, or calling their loved ones from detention. Yet the collection, storage, and use of the vast majority of surveillance data—including biometric data—will never be reviewed by any court or anyone outside law enforcement. We have seen over the last several decades that the more the right to privacy is diminished, the fewer protections people have under the Fourth Amendment, leading to a higher risk of legal system involvement, and wrongful convictions.

¹ Michigan Technological University, What is artificial intelligence (AI)?, <https://www.mtu.edu/data-science/undergraduate/ai/what-is/>

In policing, for example, where officers once relied on physical stops and interrogations, they now use surveillance technology, AI powered predictive policing algorithms, and secretive databases to track and criminalize Black and Latine youth. This shift makes it harder to challenge the basis for a stop or search in a criminal proceeding. When an officer relies on a database designation or algorithmic flag to justify a stop, search, or arrest, the database itself cannot be subjected to adversarial scrutiny, if its use is even introduced in court at all.

Further, the existence of these databases creates risk not only of misuse by third party software developers, but also of access by government agencies. Immigration and Customs Enforcement's recent uptick in obtaining and purchasing data from private entities underscores the risk of allowing the unregulated overcollection of personal data.² ICE has tracked individuals and circumvented legally required warrant practices with the express objective of facilitating deportation, as well as targeting activists.³

Tools that use AI and algorithmic decision making are being deployed across the city for monitoring, data collection, and analysis. A call to 311 or a support-hotline, a ride on the subway or in a car, or a call to a loved one in a city jail all feed private information into vast, largely-unaudited databases. Without meaningful audits, safeguards, or transparent communication about AI usage, New Yorkers are left unaware of how their data is being used—even in highly consequential, legal decision making.

NYPD's Use of AI and Algorithmic Decision Making

The NYPD is one of the City's largest users of AI-enabled software, specifically surveillance technology, while constantly evading legally-mandated transparency laws and industry-standard data privacy safeguards. Under the Public Oversight of Surveillance Technology (POST) Act, the NYPD is required to publicly post Impact and Use Policies (IUPs) for all surveillance technology. At a February 2025 hearing before the Committee on Technology, NYPD admitted to this Council that they do use artificial intelligence technology, but had yet to clarify in their IUPs how they are actually using AI and machine learning. A year later, in February 2026, the NYPD removed language from several of its IUPs—including those referencing automated license plate readers, closed-circuit television, facial recognition, data analytics tools, and other technologies—that originally stated the Department did *not* use artificial intelligence or machine learning. NYPD is choosing to parse the language around AI to sidestep meaningful transparency about the technologies it deploys and how they function.

1. The Domain Awareness System

The Domain Awareness System (DAS) is the NYPD's surveillance platform. It serves as a hub for data under the NYPD's control, aggregating all surveillance, policing, and intelligence

² Joseph Cox, *CBP Tapped into the Online Advertising Ecosystem to Track Peoples' Movements*, 404 Media (Mar. 3, 2026), <https://www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements/>

³ NPR, *ICE Has Spun a Massive Surveillance Web. We Talked to People Caught in It*, (Mar. 4, 2026), <https://www.npr.org/2026/03/04/nx-s1-5717031/ice-dhs-immigrants-surveillance-confrontation-deportation-mobile-fortify>

information which the NYPD accesses or generates—including sealed records, closed-circuit TV footage, real-time camera and sensors, and social media information, among many other data points. Officers in the field can access DAS via an application installed on their phones and tablets. NYPD officers use the app to search all of that information—for any reason—and to generate predictions based on that data.

While DAS was launched in 2008 as a counterterrorism tool, it quickly grew beyond that purpose. In a 2017 journal article, Department staff states it uses DAS to "employ a unique combination of analytics and information technology, including pattern recognition, machine learning, and data visualization"—in short, predictive policing algorithms.⁴ As artificial intelligence grew more powerful, it was increasingly paired with license plate readers, CCTV cameras, and ShotSpotter gunshot detectors to automatically flag vehicles, footage, and sounds for officers to act on.

The NYPD's appetite for data to populate the intelligence software within DAS, and to justify the overall use of this massive surveillance system, has had devastating consequences on New Yorker's civil rights and is a major driver of the mass incarceration of people of color in New York. This system has led to coercive phone seizures, social media scraping, and the mass labeling of Black and Latine youth within the NYPD Criminal Group Database (widely known as the gang database) based on association rather than conduct.

Additionally, the NYPD has a profit sharing agreement with Microsoft for the Domain Awareness System, receiving 30% of revenue of Microsoft's sales of this product to other customers worldwide.⁵ Thus, NYPD maintains a long-term profit-sharing partnership with Microsoft, the same company that is OpenAI's primary cloud partner⁶ and an investment and cloud partner in Anthropic.⁷ This past summer, Microsoft itself announced the development of their own Frontier AI models.⁸ There is currently no oversight or regulations in place to monitor or restrain NYPD's relationship with this AI giant, including what AI tools may be developed or how they could ultimately be used.

2. Patternizr

Patternizr is a predictive machine learning system developed for the NYPD beginning in 2016. The developers of Patternizr trained three separate models on "manually identified official

⁴ E. S. Levine, Jessica Tisch, Anthony Tasso, and Michael Joy, The New York City Police Department's Domain Awareness System, *Interfaces*, 47L1, 2017, <https://pubsonline.informs.org/doi/10.1287/inte.2016.0860>

⁵ Press Release, Microsoft Corp., New York City Police Department and Microsoft Partner to Bring Real-Time Crime Prevention and Counterterrorism Technology Solution to Global Law Enforcement Agencies (Aug. 8, 2012), <https://news.microsoft.com/2012/08/08/new-york-city-police-department-and-microsoft-partner-to-bring-real-time-crime-prevention-and-counterterrorism-technology-solution-to-global-law-enforcement-agencies/>.

⁶ Microsoft, *The Next Phase of the Microsoft-OpenAI Partnership*, Official Microsoft Blog (Apr. 27, 2026), <https://blogs.microsoft.com/blog/2026/04/27/the-next-phase-of-the-microsoft-openai-partnership/>.

⁷ Microsoft, NVIDIA and Anthropic Announce Strategic Partnerships, Official Microsoft Blog (Nov. 18, 2025), <https://blogs.microsoft.com/blog/2025/11/18/microsoft-nvidia-and-anthropic-announce-strategic-partnerships/>.

⁸ Julie Bort, *Microsoft Is Openly Competing with OpenAI, Anthropic More Than Ever*, TechCrunch (July 29, 2026, 5:21 PM PDT), <https://techcrunch.com/2026/07/29/microsoft-is-openly-competing-with-openai-anthropic-more-than-ever/>.

patterns,” drawing on policing data from 2006 to 2015. The model allows users to input a “seed complaint” and return ten potentially related crimes.⁹ Because the data it was trained on overrepresents Black and Latine people after a long history of racially discriminatory policing of those communities, those groups are more likely to appear as suspects and matches in the AI system today. Despite longstanding use of this AI system, Patternizr operates with very little transparency and oversight. NYPD has never published an Impact and Use Policy explicitly naming Patternizr as a law enforcement tool, despite it being available to all uniformed members of service.

3. Facial Recognition and Closed-Circuit Television (CCTV)

NYPD’s use of facial recognition technology, another form of AI, is also almost wholly opaque. Much of what the public knows about this tool comes from litigation and FOIL requests, not from any documentation published by the NYPD itself. Records obtained by the Legal Aid Society showed that 50 NYPD members had Clearview AI access after downplaying the Department’s relationship with the company.¹⁰ Because of the lack of transparency, New Yorkers have no reliable way to know when CCTV footage captured on their block has been fed into facial recognition, by whom, or with what result.

The NYPD has repeatedly claimed, including in litigation, that its cameras cannot recognize faces or identify individuals passing through a camera’s field of vision in real time. However, the Department’s choice of vendors and the nature of the cameras’ connectivity call those claims into question. To manage the various CCTV video streams, the Department contracts with Genetec, a global technology company that offers high-end AI facial recognition and video analytics integration.¹¹ Back in 2011 CCTV capability was described as a “powerful computer, using artificial intelligence [to watch] all of the cameras at once and it knows if a package has been left in one place too long.” Because the NYPD has not been transparent about whether its CCTV systems use AI and machine learning, it has been difficult for the public to rely on the Department’s assurances in this area. We urge the Council to investigate the AI tools already embedded in NYPD’s cameras and facial recognition.

4. Automatic License Plate Readers

The NYPD employs Automatic License Plate Readers (ALPRs) that capture and convert images of license plate numbers to text that can be processed and compared against existing databases of license plates of interest. Data collected by these ALPRs is retained for five years and made accessible through DAS to all uniformed members of service.¹² The massive datasets generated by these cameras are now also being combined with other public records. Now, instead of

⁹ Molly Griffard, *A Bias-Free Predictive Policing Tool?: An Evaluation of the NYPD's Patternizr*, 47 Fordham Urb. L.J. 43 (2019)

¹⁰ The Legal Aid Society, *NYPD Is Using Controversial Facial Recognition Software*, April 8, 2021.

¹¹ Genetec, Realnetworks, <https://www.genetec.com/partners/partner-integration-hub/realnetworks/facial-recognition>

¹² NYPD, *License Plate Readers: Impact and Use Policy*, February 4, 2026, https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/License-Plate-Readers-NYPD-Impact-and-Use-Policy-2.4.26-FINAL.pdf

searching for a specific license plate, law enforcement can use natural language queries that allow them to search through billions of records to find more nuanced details and patterns of behavior. This makes it possible to conduct broad, speculative searches outside of the bounds of the Fourth Amendment.

On February 4, 2026, the NYPD published an updated Impact and Use Policy for License Plate Reader (LPR) Surveillance Technology that removed a statement claiming that ALPRs do not use artificial intelligence and machine learning. Because the NYPD has not been transparent about whether its ALPR systems use AI and machine learning, it has been difficult for the public to rely on the Department's assurances in this area.

Moreover, Flock Safety has recently come to attention for its AI-enabled ALPR systems that offer a range of tools, including "Vehicle Signature" and "Convoy Search."^{13 14} These tools, respectively, allow users to identify cars by make, color, and unique characteristics and identify vehicles that are traveling together. NYPD has recently come under fire for utilizing Flock Safety's technologies to conduct more than 1,700 searches without having a contract with the company.¹⁵

5. ShotSpotter

ShotSpotter, a product of SoundThinking, is a gunshot detection technology employed by the NYPD. ShotSpotter operates through an extensive network of microphones mounted in targeted neighborhoods, predominantly in Black, brown, and low income communities, designed to detect percussive sounds and classify them as gunfire or not based on a combination of algorithmic analysis and human review. Each ShotSpotter alert triggers a system notification, dispatched automatically to NYPD's Domain Awareness System.

A NYC Comptroller audit found that ShotSpotter's classifications were accurate only 13% of the time, meaning that 87% of alerts led police to non-gunfire events, often consuming officer resources without adding meaningful safety benefits.¹⁶ Despite ShotSpotter's marketing claims, independent examinations show significant discrepancies between the system's automated classifications and human reviewer conclusions. Such limitations highlight the need for standards that require clear public notifications of AI use, along with a right to challenge flawed or harmful determinations.

SoundThinking incorporates generative AI models without naming the underlying models and without any requirements on NYPD to disclose which AI mechanisms it is deploying. For

¹³ Flock Safety, *6 Benefits of LPR for Law Enforcement* (Nov. 21, 2023), <https://www.flocksafety.com/blog/6-benefits-of-lpr-for-law-enforcement>.

¹⁴ Tom Bowman, *AI in Policing: Automatic License Plate Readers*, Ctr. for Democracy & Tech. (June 17, 2026), <https://cdt.org/insights/ai-in-policing-automatic-license-plate-readers/>.

¹⁵ Maria Cramer, NYPD Officers Used Flock Safety to Track License Plates, NY Times, (Sept. 28, 2026).

¹⁶ Office of the N.Y.C. Comptroller, *Audit Report on the New York City Police Department's Oversight of Its Agreement with ShotSpotter Inc. for the Gunshot Detection and Location System* (June 20, 2024), <https://comptroller.nyc.gov/reports/audit-report-on-the-new-york-city-police-departments-oversight-of-its-agreement-with-shotspotter-inc-for-the-gunshot-detection-and-location-system/>.

example, in June 2026 SoundThinking announced SafetySmart Field Agent, an AI layer that lets users query public safety data in natural language, drawing on ShotSpotter and related SafetySmart data.¹⁷ This new feature likely incorporates frontier AI models, but SoundThinking is not transparent about the models or vendors it uses.

If SoundThinking is already using frontier AI—and the NYPD has already spent upwards of 76 million dollars contracting with SoundThinking—then the absence of meaningful AI transparency requirements or regulatory safeguards in those contracts creates a much larger gap in oversight. There is little to prevent the NYPD from eventually using frontier AI systems directly, or from contracting with the same companies whose representatives testified before the City Council, and deploying those technologies against New Yorkers without clear disclosure, independent oversight, or enforceable limits on how they can be used.

Use of AI by the Department of Correction

Since 2014, the New York City Department of Correction (DOC) has contracted with Securus Technologies, LLC, a private prison telecommunications company, to provide phone, tablet, and surveillance services at Rikers Island and other City jails.¹⁸ That contract, currently in negotiations to be extended, has enabled Securus to amass a vast interconnected web of surveillance that is perpetually blanketing not only those presently detained in our city’s jails, but also their families, communities, and advocates. Securus houses a database of the audio recordings of every call made from our city’s jails, the transcribed text of those calls, the personal information of everyone who has been processed into those jails, and the financial information of every community member who has put money on a commissary account. That broader database operates on the indexing power of Securus’s voiceprint collection and storage. A biometric identifier, voiceprints record the arguably unique signature of a person’s speech patterns. Securus collects the voiceprints of everyone who has ever placed or received a call from the city’s jails. The company and DOC do not delete these voiceprints after a person leaves custody—even if they are found not guilty or have charges dismissed.

The data is analyzed through Securus’s flagship analytics tool, THREADS. THREADS uses AI to analyze data and generate what Securus markets as “actionable investigative intelligence.” Concretely, this means THREADS constructs social network maps showing who an incarcerated person calls, in what sequence, and how those outside contacts relate to one another; identifies a person by voiceprint across all calls in the database, including calls from facilities they have never been held in; flags unusual patterns in call volume or funding behavior; and generates automated “leads” for investigators based on communication anomalies. The company’s multiple streams of data are also actively used to train Securus’s artificial intelligence systems.

¹⁷ Press Release, SoundThinking, Inc., SoundThinking Announces SafetySmart Field Agent, the New AI Layer for Connected Platform Intelligence (June 23, 2026), <https://www.barchart.com/press-releases/2602574/soundthinking-announces-safetysmart-field-agent-the-new-ai-layer-for-connected-platform-intelligence>.

¹⁸ City of New York, Dep’t of Correction, Agreement for the Installation, Configuration and Maintenance of an Inmate Telephone System, with contractor Securus Technologies, Inc. (July 2014) (‘DOC-Securus Contract’); Amendment No. 5 to the Agreement Between DOC and Securus, signed Jan. 17, 2023.

Further, THREADS interacts with other data platforms and has integration capabilities with Palantir, the surveillance and analytics corporation building interoperable databases to track immigrants, raising concerns that jail call data could be accessible to federal immigration authorities despite New York City's sanctuary laws.¹⁹ Because of this, a call recipient who spoke to a family member at Rikers may now appear in an AI-generated ICE dossier.

NYC has the Opportunity to Meaningfully Audit and Regulate the Use of AI

We commend the Council's effort to proactively address the risks posed by AI. We strongly urge the Council to take meaningful steps to address the use of AI by city agencies that regulate and surveil the lives of New Yorkers. Common sense enforcement mechanisms and policies can be implemented to increase transparency, equity, and justice in our city.

Throughout the hearing, we heard about the importance of strong safeguards, meaningful regulation, independent audits, and third-party evaluations for AI systems. Those principles should apply just as clearly when AI technology is being used by city agencies. In 2024, Brooklyn Defenders testified before the Committee on Technology's oversight hearing on Use of Automated Decision Systems and Artificial Intelligence by New York City Agencies.²⁰ At that hearing, we testified in support three Introductions which have now become law—Int. 926 (now Local Law (LL) 193) establishing compliance standards for AI use by city agencies; Int. 199 (now LL 188) which established an Office of Algorithmic Accountability; and Int. 1024 (now LL 195) which requires the Office of Algorithmic Accountability to create a list of AI systems it for which it "conducted a pre-deployment assessment. At that hearing we offered a number of suggestions to further strengthen protections for private data and ensure public and private audits for systemic bias. It is critical that the Council holds the city accountable for establishing, staffing, and opening the office of Algorithmic Accountability. We welcome the opportunity to meet with this office to discuss our concerns about automated decision making in the family policing, immigration, and criminal legal systems.

Additionally, we encourage the council to mandate further audits of how AI tools are being used, both under policy and in practice. For example, in February 2026, Mayor Mamdani signed Executive Order 13 (EO13) which compelled six New York City agencies to audit their policies and practices related to interactions with federal immigration authorities.²¹ As a part of this audit, the EO13 Interagency Response Committee (IRC) reviewed the data sharing agreements between DOC and NYPD and their third-party technology vendors, in recognition that relying on outside vendors in an era of mass data accumulation by big tech companies and the federal government carries serious risks for immigrant New Yorkers and all New Yorkers' broader civil rights and liberties. The Interagency Response Committee indicated that they will continue

¹⁹ Maurizio Guerrero, *ICE May Still Have Massive Access to Rikers Island Data Despite City's Sanctuary Status*, Documented (July 2, 2025), <https://documentedny.com/2025/07/02/ice-may-still-have-massive-access-to-rikers-island-data-despite-citys-sanctuary-status/>

²⁰ See our testimony online here

https://bds.org/assets/images/2024_0928_Technology_AIandMachineLearning_BDS.pdf

²¹ Office of the Mayor, Executive Order No. 13, February 6, 2026, <https://www.nyc.gov/mayors-office/news/2026/02/executive-order-13>

reviewing contracts and data sharing agreements between city agencies and third parties, including agencies' compliance with the city's Identifying Information Law.²²

We encourage the Council to continue to ensure that all city agencies are auditing its use of AI tools and are in compliance with agency policies. The NYPD must be required to disclose and audit the use of their AI and surveillance tools, and independent audits of the AI tools being used by our law enforcement agencies must be done, at a minimum. No audit has been done of the underlying algorithms used by these tools, and yet the NYPD has spent tens of millions of dollars on them. Without independent testing, errors and bias baked into the training data continue to go unseen, as officers become ever reliant on these technologies.

Conclusion

We thank the Council for holding this hearing on mitigating the risks presented by Artificial Intelligence. Given the depth and reach of the city's various surveillance systems, there is an urgent need to clarify how these systems are being used, how New Yorker's privacy and civil liberties are being respected, and what audits and guardrails are in place to mitigate harm. We welcome an opportunity to speak with each of you more about the breadth of the problem we are seeing in Brooklyn and Queens and the comprehensive solutions we have begun to identify from our unique vantage point in the city.

If you have any questions or concerns, do not hesitate to contact me at jgosdigian@bds.org.

²² Administrative Code § 23-1201