NYPD

Wednesday, February 19, 2025

**STATEMENT OF MICHAEL GERBER**
**DEPUTY COMMISSIONER, LEGAL MATTERS**
**NEW YORK CITY POLICE DEPARTMENT**

**BEFORE THE NEW YORK CITY COUNCIL**
**COMMITTEES ON PUBLIC SAFETY, OVERSIGHT AND INVESTIGATIONS, AND TECHNOLOGY**
**COUNCIL CHAMBERS, CITY HALL**
**FEBRUARY 19, 2025**

Good morning Chair Salaam, Chair Brewer, Chair Gutiérrez and Members of the Council. My name is Michael Gerber, and I am the Deputy Commissioner of Legal Matters for the New York City Police Department. I am joined today by Assistant Chief Jason Savino, Commanding Officer of the Detective Bureau's Specialty Enforcement Division, and Joshua Levin, Director of Legislative Affairs for the Department. On behalf of Police Commissioner Jessica Tisch, we thank you for the opportunity to speak about the Department's compliance with the POST Act and about three pieces of legislation relating to the Department's use of surveillance technology.

Technology is critical to our public safety mission. Every day we use technology to solve crimes and to keep people safe. We are committed to using technology with care and precision, and doing so consistent with the law. When it comes to mandating disclosures regarding the Department's use of surveillance technology, there are several critical interests: transparency, public safety, innovation, and administrability. The POST Act strikes a balance between these interests, and the Department has gone to great lengths to meet its obligations under the Act. Since the passage of the POST Act in 2020, the Department has published 37 Impact and Use Policies, or IUPs. The Department has amended its IUPs 16 times—sometimes to reflect changes in policies or practices, sometimes because a surveillance technology was being deployed in a new manner or for a new purpose, and sometimes because we identified an error and acted to correct it. The IUPs are publicly available on our website and provide a wide range of information concerning the capabilities of our surveillance technologies, as well as various policies and procedures relating to those surveillance technologies.

I would like to take a moment to comment on the bills under consideration today.

**Intro. 168** would require the Department to provide to DOI, upon request, a list of all surveillance technologies, information on data access and retention policies related to those surveillance technologies, and quarterly updates on all new and discontinued surveillance technologies. The Department takes DOI's oversight mission very seriously, and provides DOI with the information that it needs to perform that role. The Department's only concern regarding Intro. 168 is the frequency of the mandated updates to DOI. Requiring updates every quarter imposes a burden on the Department that does not seem necessary for DOI to perform its annual audit function. The

Department looks forward to working with the Council to formulate a schedule for reporting to DOI that ensures that DOI has the information that it needs in a timely fashion.

**Intro. 233** would require the Department to establish and publish procedures and regulations for the use of facial recognition technology. The bill would also require the Department to conduct a biannual audit of our use of facial recognition, and to provide the results to DOI as well as publish them on our website. I would note that the Department currently posts its facial recognition policy on its website, along with answers to frequently asked questions regarding our use of facial recognition. We of course have no issue with continuing to publicize this information. We also have no objection, in principle, to providing additional data to the public regarding our use of facial recognition. The Department has had an ongoing dialogue with the Council regarding the contour and scope of the audit, and we believe that we can continue this collaboration to craft an audit that will further increase transparency regarding our use of facial recognition without impeding the use of this critical law enforcement tool.

**Intro. 480** would amend the POST Act to require, among other things, a separate IUP for each surveillance technology used by the NYPD "regardless of whether such technology overlaps in functionality or capability with any other technology" for which an IUP already exists. We are not sure what is intended by this language. At best, it is ambiguous and will lead to confusion regarding the Department's disclosure obligations. At worst, it could be read to suggest that even the slightest alteration in functionality requires a new IUP, followed by a public notice-and-comment period and a ninety-day delay before the new hardware can be used. We would need a new IUP every time we upgrade our officers' cellphones, buy a different make or model of camera, or purchase new, covert recording devices for our undercover officers. This would be very harmful to the daily functioning of the Department and could serve to compromise public safety. The Department opposes the legislation as drafted.

I would note, however, that we have been in dialogue with advocacy groups regarding proposed changes to the POST Act, in an effort to formulate revisions to Intro. 480 that will meet their concerns relating to privacy and transparency without undermining the Department's public safety efforts. That dialogue, extending over many months, has been detailed and productive, and I understand that the sponsor of the bill has been supportive of these efforts. I believe that, thanks to our work with those advocacy groups and with the Council, there is an opportunity to finalize a bill that expands the scope of the disclosure obligations under the POST Act without objection from the Department. I would add that I am proud of our efforts to work towards a compromise with groups that, to put it mildly, are harsh critics of the Department. Despite fundamental disagreements on a variety of issues, we have listened to each other and worked to identify common ground. I am hopeful that this can be a model for future dialogue.

Thank you for the opportunity to speak to these issues. We look forward to answering any questions that you may have.

Office of Technology & Innovation

**NEW YORK CITY 311 TESTIMONY BEFORE THE NEW YORK CITY COUNCIL COMMITTEES ON PUBLIC SAFETY, OVERSIGHT AND INVESTIGATIONS, AND TECHNOLOGY**

**Int 978-2024, a local law to amend the administrative code of the city of New York, in relation to requiring the 311 customer service center to provide relevant resources in response to tree pruning-related requests.**

**February 19, 2025**

Good morning, Chairs Salaam, Brewer, Gutiérrez, and members of the City Council Committees on Public Safety, Oversight and Investigations, and Technology. Please accept this written testimony on behalf of Joe Morrisroe, Deputy Commissioner of New York City 311 (NYC311), under the Office of Technology and Innovation (OTI).

As you all know, NYC311 delivers fast and easy access to government services and information to all New Yorkers. NYC311 is available 24 hours a day, 7 days a week, 365 days a year through multiple channels, including the call center, online portal, text, mobile application, and social media. Originally launched as a call center, NYC311 has evolved into the most comprehensive municipal government customer service platforms in the nation. NYC311 received 39.9 million customer contacts in 2024, and on an annual basis receives more calls than all other U.S. city 311 call centers combined.

It is important to note that NYC311 serves as the *platform* to provide information and services to the public. With few exceptions, public interactions with NYC311 services result in one of the following outcomes:

- Information Request (e.g. when is my trash pick-up day?)
- Referral to an external entity (e.g. NY State Department of Labor, FCC)
- Service Request (e.g. submitting a ticket)

We rely on our collaborative relationships with each city agency to build out the service request forms and information pages (also known as "knowledge articles") that properly reflect the mission and services for each agency or office. That said, we will provide feedback on the bill associated with this hearing.

**Introduction 978-2024** would require NYC311, in coordination with the Department of Parks and Recreation (DPR), to provide 311 customers submitting tree pruning-related service requests or information requests with certain links to certain information related to tree pruning. Having

conferred with our colleagues at DPR, we can confirm that their agency website offers a wide range of information regarding tree pruning. OTI would be able to fulfill the requirements of the legislation as it is currently drafted by aggregating existing map links and information resources from DPR. As always, we appreciate the Council's interest in continuing to improve our government's front door to information and resources, and we look forward to discussing the legislation further.

Thank you, once again, for the opportunity to submit our testimony today.

###

NEW YORK CITY COUNCIL
JOINT HEARING BY THE COMMITTEE ON PUBLIC SAFETY,
COMMITTEE ON OVERSIGHT AND INVESTIGATIONS, AND
COMMITTEE ON TECHNOLOGY

TESTIMONY OF JOCELYN E. STRAUBER
COMMISSIONER, NEW YORK CITY DEPARTMENT OF INVESTIGATION

CONCERNING OVERSIGHT OF NYPD'S IMPLEMENTATION OF THE
PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY (POST) ACT

WEDNESDAY, FEBRUARY 19, 2025

Testimony of DOI Commissioner Jocelyn E. Strauber on the POST Act
Wednesday, February 19, 2025

Good morning. My name is Jocelyn Strauber and I am the Commissioner of the Department of Investigation ("DOI"). Thank you, Chair Salaam, Chair Brewer, and Chair Gutiérrez and members of the Committees on Public Safety, Oversight and Investigations, and Technology for the opportunity to speak about DOI's oversight role with respect to NYPD's use of surveillance technology, as set out in the Public Oversight of Surveillance Technology legislation, which I'll refer to as the POST Act.

As you know, DOI oversees the operations, policies, programs and practices of the New York City Police Department ("NYPD") through DOI's Office of the Inspector General for the NYPD ("OIG-NYPD"). The POST Act requires NYPD to produce and publish Impact and Use Policies, IUPs for short ("IUPs"), for each surveillance technology used by the NYPD and directs OIG-NYPD to prepare an annual audit of the Department's compliance with these IUPs.

Since DOI last testified on this topic in December 2023, we have issued two additional reports pursuant to the POST Act. The first of those reports focused on five technologies deployed by NYPD in 2023 and the second report focused on NYPD's drone program. Today I will give you a summary of DOI's findings from those two reports and share our view of the three proposed bills under consideration today that relate to the NYPD's use of surveillance technology.

**2023 POST Act Report**

The 2023 POST Act report, issued in the spring of 2024, examined the IUPs applicable to five surveillance technologies NYPD introduced in 2023: (1) Digidog, a remotely-operated robot; (2) the Knightscope K5 Autonomous Security Robot ("K5"); (3) StarChase GPS tracking technology ("StarChase"), which allows officers to attach GPS trackers to moving vehicles; (4) IDEMIA Mobile Biometric Check application ("IDEMIA"), a smartphone application capable of collecting and comparing digital fingerprints; and (5) an augmented reality smartphone application ("the AR application"), built by NYPD's Information Technology Bureau, capable of displaying data from NYPD databases concerning a particular location when a smartphone camera is pointed at that location.

OIG-NYPD's review found that NYPD did not issue new IUPs in conjunction with the deployment of these five surveillance technologies but addressed four of them — K5, StarChase, IDEMIA, and the AR application – in five different addenda to existing IUPs in April 2023. According to NYPD, the Digidog technology was addressed in an existing IUP, issued in 2021, when an earlier version of Digidog briefly was used by the Department, and therefore no addendum was required.

OIG-NYPD concluded that as of 2024, NYPD continued to group distinct surveillance technologies within a single IUP – a practice discussed in detail in OIG-NYPD's first annual POST Act report and in my testimony before these committees in December 2023. We found that the grouping approach may shield individual technologies from public scrutiny and oversight. It is OIG-NYPD's position that the POST Act requires an IUP for each distinct surveillance technology, unless the surveillance technologies at issue are substantially similar in capability and manner of use. In that event, a single IUP may address more than one technology and should name each individual technology to which it applies.

With respect to the five technologies reviewed in the 2023 report, OIG-NYPD found that the IUPs did not include all of the information required by the POST Act. With respect to Digidog, OIG-NYPD maintained, as it did in the first annual POST Act report, that Digidog was a surveillance technology with distinct capabilities and, therefore, NYPD should have issued an IUP specific to Digidog when the technology was initially deployed in 2021. Instead, NYPD asserted that Digidog was sufficiently addressed by the IUP for Situational Awareness Cameras. We also concluded that the Digidogs purchased and deployed in 2023 had enhanced capabilities that, at a minimum, should have been addressed in an addendum to the Situational Awareness Camera IUP.

OIG-NYPD further found that the Department appropriately treated K5, StarChase, IDEMIA, and the AR application as enhancements to, or new uses of, existing surveillance technologies, and, therefore, issued addenda for each of those technologies. However, we concluded that, taken together, the IUPs and the addenda did not meet the POST Act's requirements in the following ways:

1) The Situational Awareness Camera IUP and its addenda did not disclose health and safety information with respect to K5;

2) The GPS Tracking Devices IUP and its addenda did not adequately disclose the specialized rules, processes, and guidelines that distinguish StarChase technology from other GPS tracking technologies, health and safety information, or the type of data that may be disclosed to external entities;

3) The two IUPs relevant to the IDEMIA application and their addenda did not provide sufficient information about IDEMIA with respect to policies and procedures related to data retention and access; and

4) The Portable Electronic Devices' IUP and its addenda did not provide sufficient information about the AR application regarding policies and procedures related to data retention and access.

Based on its review, OIG-NYPD issued seven policy and procedure recommendations to NYPD in the 2023 POST Act Report. The recommendations advised NYPD to issue a new IUP for Digidog and to update the addenda to the IUPs as noted above, and also to limit grouping of technologies in a single IUP to those technologies that are sufficiently similar in capability and manner of use. Two of the recommendations proposed that NYPD include mechanisms within the IUPs for tracking and monitoring uses of surveillance technologies and that each IUP should identify the potential impact of the surveillance technology on protected groups, measures that the POST Act does not require. NYPD rejected those two recommendations and accepted the remaining five.

**2024 POST Act Report**

The 2024 POST Act report focused on the NYPD's use of drones — unmanned aircraft systems ("UAS"). The Department employs drones to further search and rescue missions, disaster responses, documentation of traffic accidents and crime scenes, crowd monitoring, and for situational awareness in active shooter and hostage situations. NYPD's drone program was announced in 2018. At that time, officers assigned to TARU, the Technical Assistance Response Unit which provides NYPD with equipment and tactical support and specializes in audio/visual technology, was tasked with implementation of the program.

Since that time the NYPD's drone usage has increased. In 2023, the Department reportedly deployed drones on over 4,000 flight missions, including responding to 2,300 priority calls for service, including searches for missing people, alerts from the ShotSpotter gunshot detection system, and crimes in progress as needed. OIG-NYPD reviewed the two IUPs applicable to the drone program — the UAS IUP and the Thermographic Cameras IUP — and concluded that the Thermographic Cameras IUP satisfied the POST Act requirements with respect to the Department's use of drone technology, but the UAS IUP did not disclose all of the information required by the POST Act and did not provide a complete and accurate picture of all aspects of NYPD UAS operations in the following ways:

1) The UAS IUP inaccurately states that all drone deployments are operated and supervised by TARU, when in fact multiple units within NYPD operate their own drone programs;

2) The UAS IUP requires that the Commanding Officer of the Drone Team report to the highest-ranking uniformed member of NYPD, but in fact the Commanding Officer reports to the Deputy Commissioner of Operations, who is not the highest-ranking uniformed member;

3) The UAS IUP does not disclose several capabilities of the Department's drone fleet including features that enable fully autonomous and pre-programed flights, two- and three-dimensional mapping technologies, two-way communication capabilities, and glass breaker attachments;

4) The UAS IUP does not disclose any potential health and safety impacts of UAS, including risks related to personal injury, property damage, and the device's lithium-ion batteries, when potential health and safety risks plainly exist; and

5) The UAS IUP does not accurately reflect how NYPD maintains the logs of each drone flight.

Based on its review, OIG-NYPD issued ten policy and procedure recommendations to NYPD. Nine proposed that NYPD to update the UAS IUP to include the types of disclosures I just described, as required by the POST Act. OIG-NYPD also recommended that NYPD include in the IUP the potential impact of the surveillance technology on protected groups, which the POST Act does not require. We await NYPD's response to these recommendations which is due by March 18, 2025.

**DOI OIG-NYPD's Ongoing Role**

DOI recognizes that the use of surveillance technology in New York City raises important public concerns and we are committed to providing robust oversight in this area. Because the annual comprehensive inquiry that the POST Act requires DOI to undertake — an audit of the NYPD's compliance with each of its three dozen IUPs, for more than 80 surveillance technologies — is not feasible, we focus each annual report on particular surveillance technologies of greatest public interest and concern. We also seek to identify and to address any broader issues relevant to the POST Act's requirements and NYPD's compliance more generally, such as the grouping issue I've discussed today.

**Proposed Legislation**

DOI has reviewed Introductions 168, 233, and 480, which are being considered at today's hearing. These are bills that were first heard in December 2023, and that DOI testified about at that time. DOI continues to be generally supportive of the three bills, which track eleven of DOI's recommendations made in our 2022 POST Act report. Nine of those eleven recommendations remain rejected by NYPD. One recommendation, that NYPD issue a unique IUP for each distinct surveillance technology, was initially rejected, but was accepted after DOI reissued the recommendation in our 2023 report. Another recommendation, that NYPD provide DOI with an itemized list of all surveillance technologies the Department is using, was initially rejected, but has now been accepted in principle.

We appreciate the Council's support for our oversight mission, as well as for the specific recommendations we have made to the Department with regard to surveillance technology. We look forward to working with the Council on these bills should they move forward to a vote.

Thank you for your time and I am happy to take any questions you may have.

**PUBLIC ADVOCATE** FOR THE CITY OF NEW YORK

# Jumaane D. Williams

**STATEMENT OF PUBLIC ADVOCATE JUMAANE D. WILLIAMS
TO THE NEW YORK CITY COUNCIL COMMITTEE ON PUBLIC SAFETY,
TECHNOLOGY, AND OVERSIGHT & INVESTIGATIONS
FEBRUARY 19, 2025**

Good morning,

My name is Jumaane D. Williams, and I am the Public Advocate for the City of New York. I would like to thank Chairs Salaam, Gutiérrez, and Brewer and the members of the Committees for holding this important hearing.

In June 2020, the City Council passed the Public Oversight of Surveillance Technology (POST) Act, requiring the NYPD to disclose basic information about the surveillance tools it uses and the safeguards in place to protect the privacy and civil liberties of New Yorkers.[1] The POST Act was passed in collaboration with advocates, activists, lawyers, and civil rights groups. Under the Adams administration, the NYPD has acquired, implemented, and increased the use of numerous new technologies and tools, including drones, facial recognition technology, and different forms of surveillance cameras like the "Digidog" and the R2D2-like "K5" robot in the Times Square subway station. While this technology can be useful in protecting public safety and solving crimes, it also necessarily raises concerns about New Yorkers' civil rights, especially when the NYPD has a long history of biased policing.

Since the enactment of the POST Act, the NYPD has drawn criticism from DOI's Inspector General. Under this law, the NYPD is required to propose an Impact and Use Policy (IUP) at least 90 days prior to the use of any new surveillance technology. Any enhancements to or new uses of existing technologies require an addendum to the IUP. Last year, a report published by the OIG-NYPD stated that the NYPD's practice of grouping "surveillance technologies within a single" IUP "can limit the public transparency that the POST Act seeks to ensure."[2] The OIG-NYPD also criticized the NYPD's use of "general and generic" language used in the majority of the IUPs, such as using the term "situational awareness cameras" to describe a variety of surveillance technologies that did not receive their own specific IUPs—like the Digidog robot. This secrecy undermines transparency and accountability, leaving oversight bodies and members of the public unaware of the variety of ways the police track and surveil them.

While policing technologies can be helpful—even pivotal—in solving and preventing crimes, we know that many carry biases, just like people do. Algorithms, after all, are trained by people. One study of the efficacy of facial recognition technology has been found to misidentify Black

---

[1] https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page

[2] https://www.nyc.gov/assets/doi/reports/pdf/2024/25PostActRelease_Rpt_05_30_2024.pdf

women nearly 35 percent of the time, while it is far more accurate identifying white men.[3] Another study of Amazon's facial recognition technology mistook darker-skinned women for men 31 percent of the time, and misclassified women for men 19 percent of the time.[4] The NYPD states on their website that they use facial recognition to solve crimes,[5] but we must also recognize that this technology could also be weaponized to identify people for other purposes, such as attendees at protests who have not broken the law. The state of California recently rejected expansion for the third time in five years and US Senators have written to the Department of Homeland Security about concerns with expansion to more airports without investigation. We should take heed and carefully monitor this as the NYPD moves to do the same.

Concerns have also been raised about the use of drones; DOI found that the NYPD's IUP for drones did not "sufficiently disclose all of the information required by the POST Act, and does not provide a complete and accurate picture of all aspects of NYPD drone operations in practice."[6] For example, the IUP stated that all drone deployments are operated and supervised by the Technical Assistance and Response Unit—but DOI found multiple units within the NYPD with their own drone units.

The NYPD has been resistant to making any changes to their compliance with the POST Act, rejecting 14 out of the 15 recommendations made in the DOI report.[7] They are similarly slow to comply with other oversight measures, including responding to freedom of information requests or providing evidence to the CCRB in misconduct investigations. Dodging oversight and accountability further sows distrust between the NYPD and the community—trust that, after numerous reports about broad and biased surveillance of New Yorkers, like the Muslim community after 9/11, is tenuous and fragile.

Today several bills to strengthen the POST Act and increase transparency are being heard. Bottom line: the speed at which the Department is implementing new technologies is far outpacing their compliance to the law, this should not be. I hope that the Department listens carefully to both council and community members here today who raise concerns and call for reforms, so we can begin building that trust.

Thank you.

---

[3] https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist
[4] https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html
[5] https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page
[6] https://www.amny.com/new-york/nypd-drone-program-inspector-report-policy/
[7] https://www.brennancenter.org/our-work/analysis-opinion/nypd-continues-dodge-surveillance-transparency-laws

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

**STATEMENT OF**
**DAVID SIFFERT, LEGAL DIRECTOR**
**SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT ("S.T.O.P.")**

**BEFORE THE COMMITTEES ON PUBLIC SAFETY, TECHNOLOGY, AND INVESTIGATIONS**
**NEW YORK CITY COUNCIL**

**FOR A HEARING ON**
**UPDATES TO THE POST ACT**

**PRESENTED**
**February 19, 2025**

Good morning, Chairs Salaam, Gutierrez, and Brewer, and members of the Committees on Public Safety, Technology, and Investigations. The Surveillance Technology Oversight Project ("S.T.O.P.") is a New York-based civil rights and anti-surveillance group. S.T.O.P. advocates and litigates against discriminatory surveillance. Thanks to you and your committee staffs for organizing this hearing.

In 2020, S.T.O.P. worked alongside other advocacy organizations to fight for the passage of the Police Oversight of Surveillance Technology Act, or the POST Act. In July of 2020, S.T.O.P. submitted oral and written testimony about the importance of the legislation, specifically highlighting the impact of mass surveillance on Muslim and immigrant New Yorkers, harms from NYPD's "Gang" database, the spread of technologies such as body-worn cameras and DNA databases, and the national movement for increased transparency. Thanks to the work of countless councilmembers, advocates, and everyday New Yorkers, the POST Act passed in 2020, and it was signed by Mayor de Blasio.

The bill required New York City Police Department to disclose new surveillance technologies before implementing them. Specifically, such disclosures required a notice-and-comment process, after which NYPD would issue "Impact and Use Policies" (IUPs) for each surveillance technology. These IUPs would then be audited by the Office of the Inspector General for the New York City Police Department within the Department of Investigation.

NYPD posted its first set of 36 draft IUPs on January 11, 2021. These draft IUPs were inadequate. They lumped together different surveillance technologies under single IUPs, used boilerplate language, and failed to disclose critical information about the technologies, including information about the safety risks and disparate impact of the technologies. During the 45-day comment period, S.T.O.P. pointed out these inadequacies. However, on April 11, 2021, NYPD released its final IUPs, which were substantially similar to the drafts released in January. These IUPs failed to comply with either the spirit or the letter of the POST Act.

On November 3, 2022, OIG-NYPD released its audit of the first set of IUPs. The delay beyond statutory required deadlines was due to failure of NYPD to disclose information necessary for OIG-NYPD to evaluate the IUPs. In the audit, OIG-NYPD found that NYPD failed to comply with the spirit of the POST Act and made a series of recommendations for improving transparency.

S.T.O.P. worked with several other privacy and civil rights advocates and Councilmembers Won and Farias to introduce legislation implementing the recommendations that advocates thought would accomplish the goals articulated in the OIG-NYPD audit. Those recommendations became Intros 1207-2023 and 1193-2023 and were introduced alongside Intro 1195-2023, on which S.T.O.P. took no position.

The Council scheduled three hearings for these bills in 2023, but they were repeatedly postponed when NYPD failed to attend. During this period, NYPD updated 11 IUPs, including by adding

newly purchased surveillance robots to their "situational awareness cameras" IUP, but did not issue new ones prior to acquiring new technology.

Finally, the hearing on the POST Act updates was held on December 15, 2023 – mere days before the end of session and the expiration of the bills. At this hearing, S.T.O.P. testified to the importance of this new legislation. Meanwhile, NYPD testified that the legislation would create a slippery slope, requiring them to issue new notice-and-comment IUPs every time they upgraded any surveillance software or hardware.

In early 2024, the Council re-introduced the bills as Intros 480-2024 and 168-2024, alongside Intro 233-2024, on which S.T.O.P. again took no position. Meanwhile, conversations began with NYPD to amend the bills to clarify NYPD's requirements under them. During these negotiations, NYPD updated one IUP and issued a new IUP. Furthermore, OIG-NYPD conducted two additional POST Act audits, finding deficiencies in both. However, OIG-NYPD noted that NYPD demonstrated increased cooperation during the process.

In December 2024, after almost a year of negotiations, NYPD, advocates, and Councilmember Won agreed on wording for Intro 480-2024 that would accomplish the goals of advocates – and hopefully OIG-NYPD – while avoiding the fears of unnecessary and unproductive paperwork and labor requirements by NYPD. These amendments would also insert recommendations from OIG-NYPD's initial POST Act audit into Intro 480-2024 that had been excluded from the three bills previously, including requirements to track how surveillance data is shared. It is S.T.O.P.'s understanding that NYPD does not oppose Intro 168-2024, and S.T.O.P. takes no position on Intro 233-2024.

There are two important takeaways from this history.

First, this legislation is absolutely critical. At a time when New Yorkers are scared of the government, and the government is using information against them in countless ways, it is particularly important that New Yorkers understand exactly how they are being watched, what data is being collected, and how it is being used – before the surveillance is implemented. NYPD's existing IUPs do not accomplish this goal for reasons articulated at length by OIG-NYPD. This legislation would ensure that, going forward, NYPD's draft and final IUPs provide the notice, clarity, and transparency necessary for New Yorkers to go about their lives.

Second, over time, the nature of NYPD's engagement has changed. Both with respect to conversations with advocates and with respect to conversations with OIG-NYPD, dialogue in 2024 was far more productive than dialogue from 2021-2023. However, this does not mean that regulation is unnecessary – to the contrary, it shows how important regulation is. As individual employees and relationships change, the public's ability to access information should not. The public has a right to know how NYPD employs surveillance technology. New York City decided that when the POST Act passed in 2020, and it is all the more important in 2025. Without these POST Act updates, New Yorkers cannot get that transparency effectively and reliably.

Lastly, I would be remiss if I did not put this legislation in context. States across the country have made abortion illegal. Some have made crossing state lines for the purposes of getting an abortion illegal. They have even made shipping abortion pills from New York to their jurisdictions illegal, and a doctor has just been charged for it. They have banned gender-affirming care for minors. Many have decided that providing this health care for your child is child abuse, and unless you agree to abuse your child by withholding necessary medical care, they will take the child away. The President has sworn that he will deport millions of immigrants. The federal administration is trawling through all the data it possesses and has made it clear it intends to use that data for political purposes – to target vulnerable people or those of differing political opinions. New Yorkers are in real danger right now. If the federal government decides it wants access to any of NYPD's surveillance data, even if NYPD doesn't hand it over willingly, no provision of New York State or City law can protect against federal agents going to federal court to get a federal warrant ordering data turned over.

As a result, a few things are important. First, we need to think carefully about what surveillance data we collect. This includes the prevalence of cameras, drones, stingrays, and more. But it also includes the use of advanced technology such as facial recognition, not only by police but also by landlords and in public accommodations. Passing Intros 217-2024 and 425-2024 would ban the use of these invasive technologies and help prevent New Yorkers from being tracked.

Second, New Yorkers need to be empowered to make their own decisions. That means, we need to know what data is being collected about us and by whom. Most importantly, we need to know the data that is being collected by law enforcement. In 2025, it is more important than ever that we make sure the POST Act is up-to-date and requires the type of meaningful disclosure that the Council expected when it passed the bill in 2020.

Brooklyn Defenders

Brooklyn Defender Services
177 Livingston St, 7th Fl
Brooklyn, NY 11201

Tel (718) 254-0700
Fax (347) 457-5194
info@bds.org

**TESTIMONY OF**

**Talia Kamran, Staff Attorney,**

**Seizure and Surveillance Defense Project**

**BROOKLYN DEFENDER SERVICES**

**Presented before**

**The New York City Council**

**Committees on Public Safety, Technology, and Oversight and Investigation**

**Oversight - Examining NYPD's Implementation of the POST Act**

**February 19, 2025**

My name is Talia Kamran and I am a Staff Attorney and Equal Justice Works Fellow in the Seizure and Surveillance Defense Project at Brooklyn Defender Services. Brooklyn Defender Services (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. We are grateful to the Committees on Public Safety, Technology, and Oversight and Investigation, and Chairs Salaam, Gutiérrez, and Brewer, for inviting us to testify today about the NYPD's compliance with the POST Act.

For nearly 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 inequity. We represent approximately 23,000 people each year who are accused of a crime, facing loss of liberty, their home, their children, or 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 educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

Many of the people that we serve live in heavily policed and highly surveilled communities. These communities bear the brunt of the New York Police Department's (NYPD) privacy-destroying and abusive behavior, including through the wrongful seizure of their personal belongings, the unannounced addition of their deeply personal information (including DNA profiles, social networks, and every day habits) into unregulated law enforcement databases like

the gang database, and the unceasing subjection of "the privacies of life"[1] to police gaze through cameras, sensors, microphones, digital scraping tools, and their underlying, mass-aggregating databases like the Domain Awareness System (DAS).

The need for stringent oversight of the NYPD surveillance given this reality cannot be overstated. We are living in a city with Orwellian levels of surveillance. The NYPD has the capability—and actively uses it—to observe citizens constantly through an extensive network of CCTV cameras, as indicated in its DAS and CCTV Impact and Use Policies (IUPs). Now, with a vast array of drones equipped with audiovisual capabilities, this near-constant surveillance has become even more pervasive. This unchecked expansion of surveillance technology has serious implications for civil liberties and privacy rights, disproportionately affecting Black, brown, and low-income communities. In fact, similar practices have been found unconstitutional in other parts of the country, yet New York City continues to allow the NYPD to operate with little oversight.[2]

The Public Oversight of Surveillance Technology (POST) Act was enacted in 2020 in response to the racially discriminatory and unjustifiably invasive surveillance tactics of the NYPD, including its surveillance of Muslim communities through the use of license plate readers (LPRs) and other technologies. Despite the passage of the POST Act, the NYPD continues to evade transparency requirements and provide misleading or incomplete information about its surveillance practices. The proposed amendments—Introduction (Int.) 168, Int. 233, and Int. 480—are critical to ensuring that the NYPD is held accountable for its widespread surveillance operations. However, true oversight must also include stronger enforcement mechanisms, such as court review, to prevent continued abuse.

The NYPD has repeatedly demonstrated that it cannot be trusted to ensure its own adherence to the Constitution or to New York State and city laws. This is evident in its chronic noncompliance with other accountability and reform measures, most notably its racially discriminatory street stops, which were the subject of the *Floyd v. City of New York* litigation and ongoing federal monitoring.

As we enter the era of digital stop-and-frisk, the rights and dignity of New Yorkers are at stake. City Council must act now to strengthen the POST Act and implement other meaningful limits

---

[1] *Carpenter v. United States*, 138 S. Ct. 2206, 2213–14 (2018) ("Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted. On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure the privacies of life against arbitrary power. Second, and relatedly, that a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."

[2] *See Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 346 (4th Cir. 2021)* Holding that the Baltimore Police Department's use of an aerial surveillance system capable of tracking the movement of all residents in Baltimore while outside, and which retained data on individuals' movement for 45 days, constituted a search under the Fourth Amendment requiring a warrant in order to access to the data.

on NYPD surveillance to prevent further exacerbation of the department's already highly discriminatory practices.

**Despite minor improvements, the NYPD's IUPs lack critical information on both the privacy and legal implications of their Surveillance Technologies**

The NYPD has continually failed to comply with both the letter and the spirit of the POST Act, using broad and misleading interpretations to minimize transparency. Rather than fully disclosing the capabilities and implications of its surveillance technologies, the Department selectively omits key details regarding the most critical privacy concerns for New Yorkers.

As highlighted in the OIG's most recent report on POST Act compliance, the Unmanned Aerial Systems (UAS) IUP omits any mention of drones equipped with window-breaking technology and thermographic imaging capabilities, two technologies which raise major Fourth Amendment concerns.[3] The use of such technologies could facilitate unconstitutional warrantless imaging or entry into private residences, violating individuals' reasonable expectation of privacy as protected by the Fourth Amendment.[4] This is exactly the kind of critical information the POST Act is intended to make transparent.

Most IUPs Rules, Processes, and Guidelines sections have extremely basic boilerplate language such as the technology being used "in a manner consistent with the Constitution," without specifying concrete legal standards or limitations.[5] The fact that a practice may be Constitutional is not sufficient information to understand the wide-reaching privacy implications of said practice. For instance, the DAS IUP does not reveal to the public that DAS is used to compile entity reports on individuals, and therefore further does not inform the public as to the criteria for inclusion in the DAS. While a data dragnet that compiles information about citizens may meet some threshold of constitutionality, that does not mean it is not unduly invasive. To illustrate, through our direct client representation, BDS recently learned of an entity report in the DAS for a 5 year old child. This means that the personal information of a kindergartner, including photos and addresses, is available to any number of NYPD's 55,000 employees without any oversight whatsoever over this access. NYPD should be required to publish the criteria for the creation of an entity report—which is essentially a digital dossier—on an individual, as the current lack of transparency allows for the unchecked accumulation of personal data, including that of young children, without any public accountability or oversight.

---

[3] N.Y.C. Dep't of Investigation, DOI Report on the POST Act Release #49-2024 (Dec. 18, 2024), https://www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf.

[4] *See Id.* "the [IUP] makes no mention of this capability of certain UAS to break into a windowed structure in furtherance of this purpose. This capability allows a UAS to gain access to otherwise inaccessible areas, without obtaining a search warrant (on the basis of exigent circumstances, a legal exception to the search warrant requirement), and enables NYPD to conduct surveillance distinct from what would be visible from the naked eye. As such, the UAS IUP should be updated to disclose this capability.

[5] New York City Police Department, *Domain Awareness System (DAS) Impact and Use Policy* 4 (Apr. 9, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/domain-awareness-system-das-nypd-impact-and-use-policy_4.9.21_final.pdf

Additionally, while the DAS IUP notes that DAS itself does not use "biometric measuring technologies," DAS *has* been known to record whether the NYPD has an individual's DNA profile in their DAS entry.[6] To the extent that the NYPD has publicly discussed aspects of this technology, it has focused on the network of CCTV cameras and the Real-Time Crime Center, not on the fact that the DAS is potentially facilitating access to individuals' DNA profiles in defiance of the state law that requires all DNA profiles be stored and accessed in the state-level DNA databank.[7]

Another example is the Digital Forensic Access Tools (DFAT) IUP, which does not specify what forensic tools the NYPD possesses. Instead, the IUP speaks in broad generalizations regarding the department's various DFATs and obscures their particular capabilities. For instance, the IUP fails to mention that NYPD has a contract with GrayKey, a tool capable of brute-forcing its way into encrypted phones.[8] The IUP falsely claims that "the NYPD does not use digital forensic access tools to engage in unauthorized access or hacking,"[9] despite the fact that this is precisely what GrayKey enables.

Moreover, the IUP does not define what constitutes valid consent when an individual provides access to their device. This omission is critical when considering another DFAT the NYPD has in its arsenal, Cellebrite (which was also not specifically named in the IUP). Cellebrite's software is capable of extracting the entire contents of a phone, including metadata, call logs, and app data, yet the public remains uninformed about PD's use of this software because it is not named in the IUP.

Taken together, the omission of these two pieces of information- the lack of standards for a consent search of a technological device, as well as the use of unnecessarily invasive Cellebrite extraction software, obscures a constitutionally questionable NYPD surveillance and investigation practice. As an example, our office has seen NYPD officers coerce minors into handing over passwords under false pretenses, such as claiming they need to call a parent. Once the phone is unlocked, officers then conduct full forensic extractions, violating privacy rights and due process. Individuals subjected to these searches, minors or otherwise, are not informed of the full scope of data being extracted, making it impossible for them to provide truly informed consent.

Other IUPS similarly contain outright falsehoods, such as the cell site simulator IUP. It claims that "[c]ell-site simulators also do not capture emails, texts, contact lists, images or any other data from the device, nor do they provide subscriber account information (for example, an

---

[6] *Id.*

[7] *See* N.Y. Exec. Law § 995-C(6), requiring that DNA records collected for inclusion in the databank be kept within the state system and made available only to designated entities for *specific* law enforcement purposes.

[8] *See* Upturn**,** *Mass Extraction: The Widespread Power of Police to Search Mobile Phones (2020),* https://www.upturn.org/work/mass-extraction/ for an explanation of Graykey's capabilities.

[9] New York City Police Department, *Digital Forensic Access Tools Impact and Use Policy* 3 (Apr. 9, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/digital-forensic-accesst-tools-nypd-impact-and-use-policy_4.9.21_final.pdf

account holder's name, address, or telephone number)" - this is incorrect.[10] Both the called and calling numbers are accessible to a cell-site simulator, because this information is also available to any traditional cell tower responsible for routing the communication. Additionally, the IUP claims that "the NYPD cannot record, store, or retain any of the data processed [sic] cell-site simulators." This is also incorrect. A cell-site simulator device produced by Gladiator Forensics and used pursuant to a search warrant records a log of every communication to and from a device it targets. If they have the ability to turn this log over on discovery, they clearly have the ability to record, store, and retain the data processed by a cell-site simulator.

Finally, the Data Analysis Tools IUP is one of the most serious examples of how vague and overly broad categories can be used to prevent the public from understanding the breadth of the techniques used by the NYPD and the depth of the data sources they can draw from. This IUP is written broadly enough to cover almost any AI or machine learning tool the NYPD could deploy, yet gives only a single example of how these tools may be used to characterize this incredibly broad category: "NYPD personnel can visualize assault complaints under investigation within a particular geographic area and identify potential links between investigations using data analysis tools."

The IUP says very little about how such "potential links" are established. It could be anything among the following examples:

- "Hot spot" analysis and predictive policing that attempts to predict where crimes will occur in the future based on historical trends
- Computer vision tools that attempt to automatically classify video footage and assign labels to it, like "individual wearing a red shirt"
- Automated pattern recognition and search capabilities that allow investigators to look for words and terms that recur across seemingly disparate cases, or set up alerts for individuals or cars matching a specific description.
- Dashboards and other data displays about recent incidents in the Real-Time Crime Center.

These are just a few examples, but already give far greater specificity than the NYPD has in its disclosure. The term "Data Analysis Tool" is so broad that the NYPD could use any of the massive datasets under its control to train and deploy an AI system without disclosing its use to the public, because it would meet the technical definition of "Data Analysis Tools." Or it might mean using a language model like ChatGPT to provide a "natural language" interface to data stored in systems like the Domain Awareness System. As we know, new and untested technologies pose risks to the public when they make errors. The public should not learn about the departments' use of untested and unreliable chatbots only when the system hallucinates, or produces incorrect information about, someone's criminal history. To protect New Yorkers from unchecked and potentially dangerous surveillance expansion, NYPD should explicitly name the

[10] New York City Police Department, Cell-Site Simulators: Impact and Use Policy (Apr. 9, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/cell-site-simulators-nypd-Impact-and-use-policy_4.9.21_final.pdf.

data analysis tools they use, disclose how these tools process and interpret data, and provide clear policies on oversight and accountability.

**City Council must pass Int. 168, 233, and 480 to protect New Yorkers' civil rights and ensure proper enforcement of the POST Act**

We commend the City Council for introducing Ints. 168, 233, and 480, which would make crucial strides toward increasing transparency and oversight of the NYPD's use of surveillance technologies. However, we urge the Council to further strengthen these bills to ensure real transparency and reduce the ongoing and future constitutional harms that flow from an unchecked surveillance policing apparatus.

With respect to Int. 168, as previously discussed the NYPD relies on the same boilerplate retention policy across all of its IUPs, failing to provide meaningful details on how long data obtained through distinct technologies is stored, who has access to it, and how it may be shared. We call on the City Council to explicitly require technology-specific retention policies that provide the public with a clear understanding of how their data is handled.

Additionally, as written, Int. 168 requires the NYPD to provide an itemized list of its surveillance technologies only upon request by the Commissioner of Investigation. This places the burden of oversight on an external agency rather than requiring proactive transparency from the NYPD. Instead, the Council should mandate that the NYPD publish an itemized list of all surveillance technologies in use, ensuring ongoing public awareness and scrutiny of its ever-expanding surveillance apparatus.

Like Int. 168, 233 takes a critical step in requiring the NYPD to establish clear policies on the use of facial recognition technology. However, we urge the Council to go further by mandating that the NYPD evaluate its AI tools for racial bias. Studies have repeatedly shown that facial recognition technology disproportionately misidentifies people of color, increasing the risk of wrongful surveillance and false arrests.

The racial bias in facial recognition technology stems from the datasets used to train these AI systems. Many of these datasets are overwhelmingly composed of images of white individuals, making the software significantly less accurate when identifying people of color. A 2019 study by the National Institute of Standards and Technology found that facial recognition algorithms falsely identified Black and Asian faces up to 100 times more often than white faces.[11]

[11] P. Jonathon Phillips et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST Interagency/Internal Report (NISTIR) 8280 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

Many police departments treat AI-generated matches as definitive evidence, even when internal policies warn that the results should not be the sole basis for an arrest.[12] In several cases, law enforcement skipped critical investigative steps, ignoring alibis and even DNA evidence that contradicted AI results. Without strict oversight and requirements for independent verification, the NYPD risks using flawed technology to justify arrests, further entrenching racial disparities in the criminal legal system. The City Council must act decisively to ensure that any use of facial recognition technology is subject to rigorous bias evaluations and independent corroboration before being used to detain or prosecute individuals.

Finally, BDS supports the passage of Int. 480, a necessary step in requiring the NYPD to disclose external entities that receive its surveillance data. With that said, the language of Int. 480 can be expanded and clarified to encourage more effective transparency and compliance from the NYPD. As written, Int. 480 only mandates disclosure of who receives NYPD data, but it should also require the NYPD to list every agency and entity from which it obtains data, such as the Department of Corrections (DOC), Department of Education (DOE) and the Office of the Chief Medical Examiner (OCME). Without this full accounting, the public remains unaware of how data flows between agencies, limiting oversight and accountability.

The bill should explicitly mandate that the NYPD identify each external entity by name, detailing both the type of data exchanged and how it is gathered. For example, while the DAS IUP claims that no biometric data is included, DAS reports indicate whether an individual's DNA is on file (whether with OCME or via other systems), proving that biometric data is indirectly linked to NYPD surveillance. This lack of transparency undermines public trust and prevents an accurate assessment of NYPD data-sharing practices.

Additionally, the City Council and the Office of Inspector General (OIG) must ensure the NYPD publishes IUPs for all surveillance technologies they can access, even if those technologies are operated by external entities like the DOC or the Department of Homeland Security. Several significant tools, including Securus, THREADS, and OMNY, remain undisclosed in IUPs despite their widespread use. THREADS, for example, allows correctional staff to analyze the social networks of incarcerated individuals and create maps of individuals' social networks in and out of prisons. Individuals calling their incarcerated family members may have the data from their calls shared with the NYPD, raising the risk that they will be surveilled by the NYPD in violation of both their right to privacy as well as their First Amendment association rights. NYPD staff also have access to federal surveillance systems; excluding them from the authority of the POST Act poses the risk that the NYPD can shield their practices from scrutiny by relying upon third-party sources of surveillance data. The NYPD must be required to produce a full, itemized list of all surveillance technologies in use to prevent selective disclosure and concealment of critical information.

[12] Drew Harwell, *Police Embrace AI and Facial Recognition, Stirring Privacy Concerns*, Wash. Post (Feb. 14, 2025), https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/.

Brooklyn Defenders

**City Council Must Close the Loophole and Require Real Transparency on the Disparate Impact of NYPD Surveillance Technologies**

Finally, we urge the City Council to amend the POST Act to explicitly require the NYPD to report on the actual disparate impact of the surveillance technologies they use, rather than limiting disclosures to the theoretical impact of written policies. This distinction is critical. The public deserves transparency regarding how these tools function in practice, who is being affected, and whether they are effective in achieving their stated goals.[13]

In past POST Act audits, the Office of the Inspector General (OIG) has repeatedly recommended that the NYPD disclose the discriminatory effects of its surveillance tools.[14] However, the NYPD continues to frame its reporting around the potential disparate impact of its Impact and Use Policies (IUPs) rather than the actual consequences of the technologies themselves. This reporting failure shields the NYPD from accountability and allows ineffective and racially discriminatory technologies to remain in use.

The ShotSpotter IUP contrasted with data on the efficacy of the technology itself exemplifies why disparate impact reporting is crucial to maintaining transparency and ensuring the efficacy of surveillance tools. The NYPD claims that it does not control sensor placement, stating that ShotSpotter engineers determine locations based on gunshot data.[15] Even if this were true, the data itself is unreliable, rendering this justification meaningless. ShotSpotter's confirmation rate—the percentage of alerts verified as actual gunfire—is only 16.57 percent, and over 99 percent of alerts do not result in a firearm recovery or suspect identification.[16] Despite this abysmal performance, the NYPD continues to expand and renew its ShotSpotter contract without public scrutiny. The only reason the public is aware of these failures is due to a FOIL request and subsequent report from our office and an audit from the Comptroller[17], not because of any NYPD disclosure.

---

[13] Currently, the POST Act's disparate impact reporting requirement reads: "any potentially disparate *impacts of the surveillance technology impact and use policy* on any protected groups as defined in the New York City Human Rights Law." *Emphasis added.* N.Y.C. ADMIN. CODE § 14-188(c).

[14] City of New York Department of Investigation, *DOI'S OFFICE OF THE INSPECTOR GENERAL FOR THE NEW YORK CITY POLICE DEPARTMENT ISSUES REPORT ASSESSING NYPD'S COMPLIANCE WITH THE PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY ACT* (Dec. 2024), https://www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf.

[15] NYC Police Dep't, ShotSpotter - NYPD Impact and Use Policy (Apr. 9, 2021), https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/shotspotter-nypd-impact-and-use-policy_4.9.21_final.pdf.

[16] Brooklyn Defender Services, ShotSpotter: A Systemic Analysis of the Technology's Impact on Communities (Dec. 2024), https://bds.org/assets/files/Brooklyn-Defenders-ShotSpotter-Report.pdf.

[17] New York City 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* (Jun. 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/.

The problem is not just that ShotSpotter is ineffective. Its failures actively harm communities of color. The majority of ShotSpotter sensors in New York are placed in Black and Latine neighborhoods, meaning every time an alert is triggered—even if it is just a car backfiring—it gives officers a justification to enter these areas on high alert, often with guns drawn.[18] ShotSpotter alerts are also used to justify stopping, questioning, and frisking individuals in the vicinity, even when there is no evidence of a crime. Because of its disproportionate placement in neighborhoods with primarily Black and Latine populations, people of color disproportionately bear the burden of these unnecessary and often dangerous police encounters.

Other cities have recognized these risks. Chicago recently canceled its ShotSpotter contract after widespread concerns about its inaccuracy and racialized deployment, which contributed to the fatal police shooting of 13-year-old Adam Toledo, a child killed by officers responding to a ShotSpotter alert.[19] If the NYPD were required to disclose not just policy language but the real-world impact of its surveillance tools, City Council and the public could evaluate whether ShotSpotter and similar technologies cause more harm than good. Instead, the NYPD has avoided scrutiny, relying on unclear reporting requirements in the POST Act while continuing to deploy surveillance tools that fuel over-policing and racial profiling.

**The POST Act is a starting point. To further protect New Yorkers rights, we need better judicial and legislative guardrails**

- **Oversight of NYPD Surveillance Must Include Court Review to Ensure Constitutional Use**

City Council's oversight role–pushed forward by the POST Act's passage in 2020–currently stands alone amongst administrative and governmental checks on NYPD surveillance powers. This is so because of NYPD's failure to comply with the minimal restrictions imposed by the courts, the city's contracting and procurement processes, the city's budget choices, and the Office of Inspector General.

When it comes to the NYPD's surveillance programs, the Department does not receive any significant oversight from the courts. In its POST Act responses, the NYPD (perhaps unintentionally) revealed that, among the 36 categories of surveillance technology the Department identified, they only believe that *four* require court approval or oversight. Each of these four (two eavesdropping methods, one location tracking method, and one cell phone data extraction method) have been the subject of Supreme Court Constitutional decisions.[20]

---

[18] Brooklyn Defender Services, *supra* note 16.

[19] Martin Kaste, Chicago Mayor Drops ShotSpotter, A Gunfire Detection System, NPR (Feb. 15, 2024), https://www.npr.org/2024/02/15/1231394334/shotspotter-gunfire-detection-chicago-mayor-dropping.

[20] See Katz v. United States, 389 U.S. 347 (1967) (overturning Olmstead v. United States and holding that wiretapping, even in the absence of a physical trespass, requires a warrant); United States v. Jones, 565 U.S. 400 (2012) (holding that location tracking with a GPS device requires a warrant); and Riley v. California, 573 U.S. 373 (2014) (holding that searching and seizing the digital contents of a cell phone requires a warrant).

According to the NYPD, every other surveillance method can be deployed without any court approval or oversight.

This lack of oversight extends to warrantless seizures and searches of cell phones, a critical issue in the context of NYPD's unchecked data-gathering practices. Given the NYPD's extensive surveillance capabilities and troubling testimony from cell phone owners about the state of their devices after police seizures, there is ample reason to believe that the department is exploiting its power to seize property without a warrant as a tool for unauthorized intelligence gathering. In fact, through reviewing NYPD property vouchers for our clients' cell phones, BDS discovered that officers were entering our clients' IMEI numbers into their property tracking system. The IMEI on a phone is essentially a digital serial number which, on most models of the iPhone, can only be accessed by unlocking the phone and entering its Settings. Civil rights advocates have long worried that the NYPD records IMEI numbers in order to track individuals' movement and social media activity.[21] Worse yet, because IMEI numbers can only be accessed through unlocking most phones, simply harvesting the IMEI numbers via a search without a warrant or consent patently violates the legal precedent set in *Riley v. California*.[22] The practice of conducting IMEI searches without a warrant further underscores the need for better oversight and control over the NYPD's power to seize and retain cell phones—once a phone is unlocked, there is little to stop the NYPD from accessing far more data than what is related to the immediate investigation. The expansion of the NYPD's surveillance apparatus, coupled with its willingness to bypass legal protocols, highlights the urgent need for court oversight and clearer guidelines on the retention and use of civilian data. Citizens' devices must not be treated as indefinite sources of intelligence, and the NYPD must provide transparent and lawful justifications for retaining such devices, particularly when investigations or criminal cases have already concluded.

- **Legislative Protection for Civilian Data**

In addition to requiring warrants that reflect current technological capabilities, we must enact stronger data protection laws to safeguard citizens' privacy. The NYPD must face stricter limits on the duration of data retention and be held accountable for how this data is used, ensuring that information is not misused or stored indefinitely without due process. Civilian privacy and constitutional rights should never be secondary to the unchecked power of law enforcement.

Data should be protected similarly to DNA, as both contain highly sensitive, identifying information. New York Executive Law §995-c, which governs the state's DNA identification index, provides a framework for how sensitive data should be handled, setting important precedents for data privacy, retention, and sharing. For instance, DNA records are only released

---

[21] Graham Rayman, *NYPD seeks to grab cell phone IDs from people under arrest or in custody; push for IMEI numbers raises concerns*, Daily News. https://www.nydailynews.com/2023/07/08/nypd-seeks-to-grab-cell-phone-ids-from-people-under-arrest-or-in-custody-push-for-imei-numbers-raises-concerns/.

[22] *See Riley v. California*, 573 U.S. 373 (2014), holding held that police must obtain a warrant before searching digital information on a cellphone seized from an arrestee, as the search-incident-to-arrest exception does not apply to modern cellphones due to their vast storage capacity and the privacy concerns involved.

under strictly defined circumstances, such as to law enforcement agencies through written agreements or to defendants for their legal defense. Civilian data collected through surveillance technologies should be subject to similar constraints to prevent indiscriminate sharing and misuse.

Furthermore, Executive Law §995-c includes provisions for data expungement, ensuring that DNA records are removed when convictions are overturned or charges are dropped. A similar mechanism must be established for digital data collected by the NYPD, allowing individuals to request the deletion of their personal information if it was gathered without legal justification or if the associated case does not result in prosecution. Without such safeguards, New Yorkers face indefinite retention of their personal data with little recourse.

**Conclusion**

The NYPD has demonstrated time and again that it will resist transparency measures unless forced to comply. Without aggressive enforcement, enhanced legislative protections, and court oversight, the Department will continue to expand its unchecked surveillance power, deepening existing inequities in policing and eroding fundamental civil liberties.

As Professor Andrew Ferguson noted before the United States Congress in 2019, "the Fourth Amendment will not save us from the privacy threat posed by [surveillance] technolog[ies]. The Supreme Court is making solid strides in trying to update Fourth Amendment principles in the face of new technology, but they are chasing an accelerating train and will not catch up. Legislation is needed to respond to the real-time threats of real-time technology."[23] The burden now falls on legislative bodies, including the City Council, to enact meaningful reforms before these technologies become even further embedded in the daily lives of New Yorkers.

Unchecked surveillance does not equate to safety. It increases government overreach, fuels discriminatory policing, and diminishes the freedoms of those who already face systemic oppression. The City Council must act now to close loopholes, impose stricter oversight, and ensure that the POST Act is a meaningful tool for accountability. We urge the Council to pass Int. 168, 233, and 480, implement additional protections against surveillance abuses, and hold the NYPD accountable to the communities it is meant to serve.

If you have any questions, please do not hesitate to contact Jackie Gosdigian, Senior Policy Counsel, at jgosdigan@bds.org.

[23] Andrew Guthrie Ferguson, "Written Testimony of Professor Andrew Guthrie Ferguson before the House of Representatives Committee on Oversight and Reform," Hearing on Facial Recognition Technology: Its Impact on our Civil Rights and Liberties (May 22, 2019).

Testimony on NYPD's Implementation of the Public Oversight of Surveillance Technology (POST) Act

- Int 0168-2024 The department of investigation's oversight of the police department use of surveillance technology.
- Int 0233-2024

  The establishment of a police department policy for using facial recognition technology and regular audits to ensure compliance.

- Int 0480-2024 Police department transparency in the use of surveillance technology.
- Int 0978-2024 Requiring the 311 customer service center to provide relevant resources in response to tree pruning-related requests.

Wednesday, February 19th
New York City Hall

Good afternoon, members of the New York City Council.

My name is Thomas Gilbert, and I am the Founder & CEO of Hortus AI. I am here representing Hortus's mission to empower local communities to assess and integrate AI technologies on their own terms.

Precisely one hundred years ago, Robert Moses set up shop at 302 Broadway, overlooking City Hall. Through a combination of graft, incentives, cunning, and deceit–most of it legal–Robert Moses rebuilt New York City in his own image, under the aegis of public safety. And he did it through surveillance. Opposing Moses, Jane Jacobs wrote that a street needs three things in order to be safe. First, a street must have a *clear separation between public and private*. Second, it must have the watchful *eyes* of storekeepers, residents and those passing by. Third, a sidewalk is needed so that people can use the street *regularly*, even without cars.

In other words, streets are not made safe by technology, but by having certain clearly-defined properties: as public, as watched, and as regularly used. Moses thought surveillance could make the public safe, but Jacobs knew it was the other way around.

Today, the Committee on Technology is considering how to more clearly implement the Public Oversight of Surveillance Technology (POST) Act. The three pieces of legislation introduced by council members Amanda Farías, Crystal Hudson, and Julie Won are not just good ideas. They respectively enact Jacobs' three criteria for safety. 0168-2024 would require the NYPD to evaluate and report on the private surveillance technologies it uses for public benefit. 0233-2024 would require regular, written audits of the NYPD's use of facial recognition technology, and to

widely share the audits' findings. 0480-2024 would ensure continuous transparency in NYPD's required "Impact and Use" criteria.

These proposals reflect a growing awareness that AI technologies are not safe because they can learn from data, or recognize faces, or are managed by technocrats. Rather, AI systems are safe because of their commitments to and from public interests.

Emerging forms of AI like chatbots will require even more intensive forms of oversight, regular audits, and substantive transparency. Hortus's work is designed to address this. Alongside our work with the public sector, Hortus has outlined what is toxic about AI today–prioritizing business objectives over quality of life and impacts on communities–and how it could be built differently. Hortus solves this by providing tools to government entities to implement AI for active citizens, in partnership with local institutions.

In tandem with the proposed Office of Algorithmic Data Integrity, we hope to work with New York City officials and propose more progressive audit frameworks for AI systems, from facial recognition to generative AI applications. I invite members of the City Council and my fellow citizens to join in this work to ensure that oversight of AI systems is of, by, and for the people.

Thank you for your attention.

Thomas Krendl Gilbert
Founder & CEO, Hortus AI
tom@hortus.ai
[redacted]

**Testimony of Michael Sisitzky**
**On Behalf of the New York Civil Liberties Union**
**Before the New York City Council Committees on**
**Public Safety, Technology, and Oversight and Investigations**
**Regarding the NYPD's Implementation of the POST ACT**

**February 19, 2025**

NYCLU
ACLU of New York

125 Broad Street
19th Floor
New York NY 10004
(212) 607-3300
nyclu.org

Donna Lieberman
*Executive Director*

Wendy Stryker
*President*

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the implementation of the Public Oversight of Surveillance Technology ("POST") Act and the compliance – or lack thereof – with the law's requirements by the New York Police Department ("NYPD" or "Department"). The NYCLU, the New York affiliate of the American Civil Liberties Union, is a not-for-profit, non-partisan organization with eight offices throughout the state and more than 85,000 members and supporters. The NYCLU's mission is to promote and protect the fundamental rights, principles, and values embodied in the Bill of Rights of the U.S. Constitution and the New York Constitution.

A core component of our work is protecting New Yorkers' rights to be free from discriminatory and unwarranted surveillance by law enforcement. Left unchecked, police surveillance has the potential to chill the exercise of First Amendment-protected speech and religious worship, intrude on Fourth Amendment-protected privacy rights, and cast entire communities under a cloak of suspicion in contravention of the Fourteenth Amendment's guarantee of equal protection.

The POST Act was passed in 2020 in response to the NYPD's long and troubling history of engaging in surveillance tactics that target political dissent, criminalize communities of color, and jeopardize all New Yorkers' privacy. Despite years of assurances from the NYPD to the contrary, the City Council recognized the obvious fact that the NYPD cannot be trusted to monitor its own use of surveillance technologies or be allowed to keep the full extent of its surveillance infrastructure secret from the public and policymakers alike.

The law's mandate is simple: the NYPD is required to disclose the technologies currently in its possession and that it intends to deploy in the future, along with the policies that govern their use. The information required to be made public under this law is the baseline information needed to evaluate the ways in which NYPD surveillance practices: target communities of color; magnify discrimination in areas like immigration, housing, and education; and contribute to our continued overinvestment in and militarization of law enforcement.

NYCLU
ACLU of New York

125 Broad Street
19th Floor
New York NY 10004
(212) 607-3300
nyclu.org

Donna Lieberman
*Executive Director*

Wendy Stryker
*President*

Despite this clear, straightforward mandate, the NYPD – which was loudly on record in its opposition to the passage of the POST Act[1] – has fallen far short of compliance. The Department published its first draft surveillance technology impact and use policies ("IUP") on January 11, 2021, finalizing them – largely unchanged – on April 11, 2021, after a public comment period. As the NYCLU noted in our comments at the time,[2] the policies reflected a lazy, copy-and-paste approach, incorporating boilerplate language throughout and obscuring or withholding baseline information needed for a full review of and understanding of how the NYPD's surveillance infrastructure operates.

Indeed, in its first assessment of the NYPD's compliance with the POST Act, the Office of the Inspector General for the NYPD ("OIG-NYPD") concluded that the policies lacked sufficient detail to enable the Office to conduct the audits required of it under the legislation,[3] frustrating both the initial transparency goals of publishing policies in the first place and preventing any meaningful oversight of those policies and surveillance practices going forward.

Then, as now, the policies give no meaningful consideration to potential disparate impacts arising from the use of surveillance technologies. Instead, most policies simply include a recitation of the NYPD's purported commitment to impartial law enforcement and its prohibitions on bias-based profiling. OIG-NYPD's report notes that the NYPD, in an attempt to justify this more limited approach, interprets the POST Act to only require consideration of potential disparate impacts regarding the use of the Department's impact and use *policies*, as opposed to the *use* of the technology actually covered under such policies.[4] But to the extent that the POST Act's language mandates that the policies themselves must also explicitly cover the "rules, processes and guidelines . . . regulating access to or use of such surveillance technology … [and] policies and/or practices relating to the retention, access and use of data collected by such surveillance technology. . . "[5] it is self-evident that the POST Act's requirement to assess potentially disparate impacts encompasses an analysis of how the rules and procedures contained within these policies are operationalized in practice.

At minimum, the Department owes the public a basic acknowledgement of the risks of disparate impacts arising from its surveillance practices and an explanation of any efforts to mitigate those risks. Instead, the NYPD's policies

---

[1] Alan Feuer, *Council Forces NYPD to Disclose Use of Drones and Other Spy Tech*, N.Y. Times, June 18, 2020, https://www.nytimes.com/2020/06/18/nyregion/nypd-police-surveillance-technology-vote.html.
[2] NYCLU, *Comments on Draft Surveillance Impact and Use Policies*, Feb. 24, 2021, https://www.nyclu.org/sites/default/files/field_documents/nyclu_letter_on_post_act_draft_policies_0.pdf [hereinafter NYCLU Comments].
[3] OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD, AN ASSESSMENT OF NYPD'S RESPONSE TO THE POST ACT, NYC DEP'T OF INVESTIGATION 4 (2022), https://www.nyc.gov/assets/doi/reports/pdf/2022/20PostActRelease_Rpt_11032022.pdf [hereinafter FIRST OIG-NYPD REPORT].
[4] *Id.* at 34.
[5] *See* N.Y.C. Admin. Code § 14-188.

on facial recognition and its criminal group database downplay documented instances of racial bias. And its policies on tools like ShotSpotter and license plate readers focus so narrowly on the supposed incapability of the technologies themselves to discriminate that they ignore the context in which such technologies are deployed – namely, a history of disproportionately placing such technologies in communities of color. A license plate reader may scan plates irrespective of the demographic profile of a vehicle's driver, but when these readers are deployed outside mosques as the NYPD has done in the past,[6] it is clear that their use has the very real potential to more aggressively target particular communities.

The NYCLU's analysis and OIG-NYPD's report also found the NYPD's reporting on data retention and sharing practices to be deficient. The NYPD's policies simply suggest that other government agencies may have access to NYPD data, without naming such agencies. Nor do the NYPD's policies describe the type of information or data being disclosed to those entities or the safeguards and restrictions – if any – imposed on those entities when the NYPD shares such data.[7] Further, when it comes to data retention, the NYPD defaults to boilerplate language on its compliance with retention schedules without shedding any real light on just how long the Department is holding on to New Yorkers' sensitive information. Knowing who has access to our sensitive data and what protections exist to prevent misuse is all the more critical with a new Trump administration that has promised to weaponize data collection and information-sharing as they target political opponents, immigrant communities, and others.

Other aspects of the NYPD's policies were, troublingly, outright inaccurate or misleading. The NYPD's initial draft policies for ShotSpotter, for example, claimed that the technology made no use of artificial intelligence or machine learning, despite the fact that ShotSpotter's official website devoted an entire section to "Artificial Intelligence and Machine Learning" on its "Technology" landing page. And the Department's initial facial recognition policy similarly suggested that no artificial intelligence or machine learning would be used, despite the fact that these systems rely on exactly those mechanisms as a basic function. Rather than correct these inaccuracies following public comment, the NYPD simply revised their policies to remove any references to the use of artificial intelligence or machine learning, turning policies that contained falsehoods into policies now replete with omissions.

Perhaps the most obvious shortcoming of these policies, however, is evident in the Department's approach to identifying the technologies themselves. The policies released by the Department consist of vague, overbroad groupings of discrete surveillance technologies that – in the NYPD's view – share sufficient similarities and general capabilities to allow for their grouping together into one overarching policy. The result is that, contrary to the purpose of the POST

[6] *NYPD Defends Legality of Spying on Mosques*, CBS News, Feb. 24, 2012, https://www.cbsnews.com/news/nypd-defends-legality-of-spying-on-mosques/.
[7] *See* NYCLU Comments at 4.



NYCLU
ACLU of New York

125 Broad Street
19th Floor
New York NY 10004
(212) 607-3300
nyclu.org

Donna Lieberman
*Executive Director*

Wendy Stryker
*President*

Act, the public did not learn the specific tools in the NYPD's surveillance arsenal, and were instead presented with categories of tools devoid of nuance. This approach flies in the face of the plain language of the POST Act. As the first OIG-NYPD report noted, "the most logical reading of the POST Act's language is that it requires an IUP for each surveillance technology," pointing to the statutory text that specifically uses a singular noun in requiring the NYPD to develop an IUP with respect to "*a* surveillance technology," indicating a clear intent to treat each such technology separately.[8] The grouping together of these technologies made it impossible for OIG-NYPD to assess whether the actual use of discrete technologies complied with the underlying IUPs.[9]

And the report – rightly – predicted a disturbing possibility from such groupings, namely that this approach "could allow NYPD to introduce new technologies under an existing group category covered by an existing IUP, and begin use immediately without the required notification to the public and City Council."[10] Because only new policies – and not enhancements to existing ones – require notice and comment periods, an IUP broad enough to capture completely new and unanticipated surveillance technologies would serve as a shield against the law's clear transparency goals. The April 2023 announcement by the Mayor and the NYPD that the Department would once again be using the so-called "Digidog," in addition to the K5 Autonomous Security Robot and StarChase GPS tagging systems was a clear example of how the NYPD has used these broad IUP categories to evade its reporting obligations.[11] The NYPD did not initially issue individual IUPs for any of these technologies. Despite the fact that they have capabilities separate from each other and from existing tools utilized by the NYPD, the Digidog and K5 robot were merely incorporated as enhancements to the IUP for situational awareness cameras, and the StarChase system was incorporated as an enhancement to the general policy on GPS devices.[12]

OIG-NYPD's first report made 15 recommendations for the NYPD to consider, including that the NYPD: issue individual IUPs for each technology, explicitly name the agencies outside the Department with whom the NYPD shares data, consider the disparate impacts from technologies themselves and not just from the implementation of the IUPs, specifically consider health and safety hazards in their use of these technologies, and create an internal tracking system for every instance in which data is shared externally, among others.[13]

OIG-NYPD's second report focused on the technologies, discussed above, announced in April 2023 that did not undergo a public notice and comment

[8] FIRST OIG-NYPD REPORT at 36.
[9] *Id.*
[10] *Id.*
[11] *See* Annie McDonough, *NYPD May Be Violating Police Surveillance Transparency Law*, City & State NY, April 13, 2023, https://www.cityandstateny.com/policy/2023/04/nypd-may-be-violating-police-surveillance-transparency-law/385173/.
[12] *Id.*
[13] FIRST OIG-NYPD REPORT at 37-39.

NYCLU
ACLU of New York

125 Broad Street
19th Floor
New York NY 10004
(212) 607-3300
nyclu.org

Donna Lieberman
*Executive Director*

Wendy Stryker
*President*

period because the Department simply updated existing policies rather than issue new ones. The report specifically criticized the Department for its failure to issue an individual policy governing the use of the Digidog, while also finding that the NYPD did not accurately describe its capabilities in its update to the situational awareness camera policy.[14] That report restated the recommendation that NYPD limit its approach to grouping different technologies together and called on the NYPD to review its existing policies to determine whether or not to separate out discrete technologies into their own policies.[15] While the Department claimed to have accepted the recommendations to issue a separate policy covering the Digidog, end overbroad groupings, and to review existing policies,[16] it does not appear to have taken steps to implement those recommendations based on the policies currently listed on its POST Act landing page.

NYCLU
ACLU of New York

125 Broad Street
19th Floor
New York NY 10004
(212) 607-3300
nyclu.org

Donna Lieberman
*Executive Director*

Wendy Stryker
*President*

The most recent OIG-NYPD POST Act report, issued in December 2024, focused on the NYPD's policy governing the use of unmanned aircraft systems ("UAS" or, more commonly, "drones"). That report found that the NYPD's use of drones has increased dramatically, from 119 drone deployments in 2019 to 540 in 2023 and an eye-popping 2871 deployments through the end of the third quarter of 2024.[17] It also found – among other issues – that the NYPD's policy failed to accurately describe the units that have the ability to operate drones, omitted key capabilities of the technology, and lacked consideration of potential health and safety impacts.[18] The report further noted that OIG-NYPD was unable to fully assess whether the NYPD's use of drones complied with the impact and use policy because the NYPD failed to provide the full scope of records requested by OIG-NYPD.[19] The report made a number of recommendations primarily focused on remedying these deficiencies.

Frome these three reports, it is clear that further action by the City Council is needed to address these issues and to bring the NYPD into compliance with the original intent of the POST Act. The overbroad groupings and boilerplate language on data retention and sharing practices and disparate impacts that have characterized the NYPD's impact and use policies thus far undermine the POST Act's transparency goals. Without City Council action, New Yorkers may be left in the dark when it comes to details on the specific surveillance

---

[14] OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD, AN ASSESSMENT OF NYPD'S COMPLIANCE WITH THE POST ACT, NYC DEP'T OF INVESTIGATION 14 (May 2024), https://www.nyc.gov/assets/doi/reports/pdf/2024/25PostActRelease_Rpt_05_30_2024.pdf.
[15] *Id.* At 41-42.
[16] MICHAEL GERBER, NYPD RESPONSE TO AN ASSESSMENT OF NYPD'S RESPONSE TO THE POST ACT, NYPD (2024), https://www.nyc.gov/assets/doi/oignypd/response/NYPD%20Response%20to%20Post%20Act%20Report_9272024.pdf.
[17] OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD, AN ASSESSMENT OF NYPD'S COMPLIANCE WITH THE POST ACT, NYC DEP'T OF INVESTIGATION 16 (Dec. 2024), https://www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf
[18] *Id.* at 6.
[19] *Id.*

technologies deployed in our communities. It is all the more urgent that the City Council act, given the Adams' administration's intense focus on expanding the NYPD's technological and surveillance capabilities and given the public's justified concerns about the ways in which the Trump administration may seek to acquire and weaponize our sensitive data.

The City Council originally passed the POST Act because it was clear that the NYPD could not be trusted to police itself and that basic transparency over its surveillance practices and abuses was a matter of vital public concern. The NYCLU supports Intros. 168 and 480, which speak to those same concerns and that would effectively codify many of the recommendations from OIG-NYPD's report.

NYCLU
ACLU of New York

125 Broad Street
19th Floor
New York NY 10004
(212) 607-3300
nyclu.org

Donna Lieberman
*Executive Director*

Wendy Stryker
*President*

Intro. 480 would explicitly name the outside entitles who have access to NYPD surveillance data, require a better accounting of the safeguards to protect against further dissemination of that data, clarify that the NYPD must consider the potential for disparities from the use of the technologies themselves, and clearly mandate that the NYPD issue discrete IUPs for each separate surveillance technology rather than grouping supposedly overlapping technologies together. Intro. 168, meanwhile, would ensure that OIG-NYPD has access to the additional information it needs to carry out its mandate, including by requiring the NYPD give the Office an itemized list of all surveillance technologies used by the Department, more detailed information on data access and retention practices, and quarterly updates to OIG-NYPD on any new or discontinued uses of technologies or changes to data access and retention policies. While the scope of the NYPD's reporting obligations were always clear, to the extent that the NYPD has sought to poke holes in the POST Act, these bills would take an important step toward closing them. The NYCLU supports these proposals and looks forward to working with the Council to incorporate additional reforms, including the recommendation from OIG-NYPD to more fully consider any health and safety risks related to the use of particular surveillance technologies.

We must also emphasize that, while transparency and oversight are critically important, transparency for transparency's sake is not and never was the sole purpose of the POST Act. Rather, the transparency provided through the POST Act – and these bills, which seek to strengthen and clarify the Act's original intent – must inform broader public consideration of the ways in which particular surveillance practices deserve closer regulation or outright prohibitions. Technologies like facial recognition, for example, have no business being used by the NYPD, and the NYCLU calls on the City Council to introduce and pass legislation that would put an end to the Department's use of this biased and flawed technology, along with other forms of biometric surveillance by police and government agencies.

The NYCLU thanks the Committees for the opportunity to provide testimony and look forward to working with the Council on these critical issues in its next term.

Testimony of

Sergio De La Pava

Legal Director

New York County Defender Services

Before the Committees on Public Safety, Oversight and Investigation, and Technology

Oversight Hearing Examining the NYPD's Implementation of the POST Act

February 19, 2025

My name is Sergio De La Pava and I am the Legal Director at New York County Defender Services (NYCDS). We are a public defense office that every year represents New Yorkers in thousands of cases in Manhattan's Criminal, Supreme, and Family Courts. Thank you to Councilmembers Salaam, Gutiérrez, and Brewer for holding this hearing on the NYPD's implementation of the POST Act, which in 2020, imposed important transparency requirements on our city's police force.

## 1. Background

In the summer of 2020, New York City passed the Public Oversight of Surveillance Technology (POST) Act, which required the NYPD to disclose to the public basic information about the types of surveillance technology that they use in New York City.

In the years preceding the bill's passage, the NYPD secretly invested billions of taxpayer dollars purchasing private, military-grade surveillance systems to closely monitor New Yorkers. The breadth of the police surveillance operations was unprecedented. The NYPD installed license plate readers throughout our streets, bridges, and tunnels, and deployed facial recognition

technology to scan social media, the department's own internal database of mugshots, and the vast network of surveillance cameras in our subway system and across the city. Yet, prior to the passage of the POST Act, there were no oversight or reporting requirements to track the NYPD's use of this unprecedented surveillance technology.

For most New Yorkers, the widespread deployment of these technologies raises grave invasion of privacy concerns and valid fears of censorship. For public defender offices like NYCDS, the NYPD's surveillance operations pose deeper questions about the reliability of these technologies, and profound 4th amendment constitutional concerns. The dramatic arrest of our client, Derrick Ingram, in 2020, described below, illustrates the serious potential for abuse and personal retaliation in the NYPD's unchecked use of surveillance technology.

The POST Act was an effort to bring some measure of oversight, transparency, and accountability to the NYPD's vast surveillance operations. The POST Act requires the NYPD to publish Impact and Use Policies ("IUPs") at least ninety days prior to deploying any new technology and to consider public comments prior to its use. The IUP must include, at a minimum, a description of the technology, as well as accompanying procedures designed to prevent unauthorized use, ensure legal privacy protections, and safeguard sensitive information. The legislation also authorizes the NYS Office of the Inspector General to conduct regular audits of the NYPD's technology and report on its compliance with the law.

In the years since the passage of the POST Act, the NYPD's surveillance operations have significantly expanded, yet its compliance with the reporting and transparency requirements have been woefully inadequate. According to OIG Audits from November 2022, May 2024[1], and December 2024, the NYPD has only minimally reported on its surveillance operations in contravention of the statute's significant requirements, found loopholes in the statute that allowed it to "group" technologies together to evade scrutiny, and otherwise failed to provide the level of transparency needed to ensure public confidence.[2]

What little information has been disclosed has only raised more questions than answers. And, more alarmingly, it reveals highly undisciplined practices that are out of step with industry standards. For example, in the 2022 OIG report, the NYPD admitted to routinely modifying source images in its facial recognition scanning operations, but doing so without any internal

[1] Strauber, Jocelyn E. "Doi's Office of the Inspector General for the NYPD (OIG-NYPD) Issues Report Assessing NYPD's Compliance with the Public Oversight of Surveillance Technology (POST) Act." *The City of New York Department of Investigation*, May 2024, www.nyc.gov/assets/doi/reports/pdf/2024/25PostActRelease_Rpt_05_30_2024.pdf

[2] Strauber, Jocelyn. "DOI's Office of the Inspector General for the New York City Police Department Issues Report Assessing NYPD's Compliance with the Public Oversight of Surveillance Technology Act." *The City of New York Department of Investigation*, Dec. 2024, www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf

policy guiding the image modification practice and without even requiring documentation of the alterations that were made. Moreover, OIG found that some source images were modified by using Microsoft Paint, an amateur graphics editing tool, rather than any professional software.[3]

Subsequently, the May 2024 OIG report revealed that the NYPD had also failed to comply with POST Act reporting requirements related to its use of the infamous, highly controversial "Digidog." And in the December 2024 POST Act audit, the OIG found that the NYPD had not adequately disclosed information related to its use of drones, despite rapidly expanding these operations in recent years. Notably, this has become an area of grave public concern.[4]

These examples illustrate the need for more robust reporting and disclosure requirements, as well as clear guidance from our city government that define and limit the NYPD's use of these tools.

2. **The misuse of surveillance tools in the 2020 arrest of a NYCDS client is a cautionary tale.**

In the summer of 2020, NYCDS represented a Black Lives Matter protester, Derrick Ingram. His high profile, dramatic arrest serves as a powerful example of the high potential for abuse inherent in these surveillance technologies.

Months before his arrest, Mr. Ingram attended a demonstration organized to protest and mourn the murder of George Floyd and, according to the NYPD, yelled into a megaphone near an officer. In response, and with the assistance of facial recognition software, intercepted phone calls, and drones that peered into his bedroom window, the NYPD tracked down the identity and home address of Mr. Ingram. On a Friday morning that August, helicopters, snipers, drones, police dogs, dozens of police vehicles, and countless officers dressed in tactical gear descended on his Hell's Kitchen apartment. Despite having no warrant for Mr. Ingram's arrest, the Department blocked Mr. Igram's entire street and terrorized his neighborhood for hours.

This incident provides a stark illustration of the dangers of unchecked police surveillance operations. After the incident, then-Mayor De Blasio admitted that the militarized operation was not authorized by NYPD leadership.[5] Indeed, in the absence of public oversight and strict

---

[3] Strauber, Jocelyn, and Jeanene Barrett. "Assessment of NYPD's Response to the Post Act." *New York City Department of Investigation Office of the Inspector General for the NYPD (OIG-NYPD)*, 2022, www.nyc.gov/assets/doi/reports/pdf/2022/POSTActReport_Final_11032022.pdf

[4] Betts, Anna. "New Report on New York Police's Drone Operations Released amid Sightings." *The Guardian*, Guardian News and Media, 18 Dec. 2024, www.theguardian.com/us-news/2024/dec/18/new-york-police-drone-capability-report

[5] Folley, Aris. "NYPD Used Facial Recognition Software during Investigation Targeting Black Lives Matter Activist." *The Hill*, The Hill, 19 Aug. 2020, thehill.com/policy/technology/512729-nypd-used-facial-recognition-software-during-investigation-targeting-black/

protocols governing the use of surveillance technologies, these tools were ostensibly manipulated by rogue officers to pursue personal vendettas. As a Retired NYPD Sergeant Detective put it, "[i]f you don't wanna get hunted down by the police, don't be yelling in cops' ears with bullhorns."[6]

Even the usual demands of criminal court process were not enough to pierce the veil of secrecy NYPD maintained surrounding its use of controversial technologies against Mr. Ingram. NYCDS's investigation into the scale and scope of the use of police technology was repeatedly stymied during the life of Mr. Ingram's criminal matter. Repeated demands by Mr. Ingram's counsel for evidence related to the raid went ignored, and countless questions remain surrounding when and how such a large-scale operation was authorized, and which precise technologies were employed.

3. **The POST Act should be amended to fortify NYPD's reporting and disclosure requirements of its surveillance operations.**

NYCDS supports the assessment of the OIG that the POST Act must be amended to close current loopholes and fortify its reporting and disclosure requirements.

Specifically, we support Int 0168-2024, a bill sponsored by Council Member Farias which would require that on a quarterly basis and upon request the NYPD provide the DOI with an itemized list of all surveillance technologies currently used or newly acquired by the Department. In addition, it would wisely require that the NYPD provide information on all data access and retention policies for data collected by such technologies. Currently, as reported by the OIG audits, the NYPD fails to provide detailed descriptions of its data retention policies and relies instead on boilerplate language. This proposed amendment to the POST Act would require the NYPD to provide more robust reporting on how it handles and stores the sensitive, private information that it obtains through these surveillance technologies.

In addition, NYCDS supports Int 0480-2024, a bill sponsored by Council Member Won which would close loopholes in the POST Act and require more specific reporting on surveillance technologies. Importantly, the bill proposes an amendment to the IUP reporting mandate that would require the NYPD to report on *every* new technology used in surveillance operations, even if analogous technologies have been previously reported on. As noted in the December 2024 OIG audit, the NYPD has previously avoided publishing IUPs for new generations of technologies with heightened capabilities by alleging that the POST Act only requires an initial

[6] Joseph, George, and Jake Offenhartz. "NYPD Used Facial Recognition Technology in Siege of Black Lives Matter Activist's Apartment." *Gothamist*, 2020, gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment

reporting on the earliest version of the tool.[7] In the instance cited in the December 2024 OIG report, while the NYPD did publish an initial IUP on its use of drones in 2021, along with an update in 2023, the NYPD failed to report its use of a new class of highly sophisticated, military-grade drones, which were equipped with thermal imaging, 3-D mapping capabilities, and glass breaker attachments that allow the vehicles to enter private buildings. The public clearly has an interest in learning about heightened features of existing technology. City Council should close the loophole that allows the NYPD to evade public scrutiny of subsequent generations of these devices by simply relying on an earlier generation's IUP.

4. **The POST Act should be amended to codify best practices in the use of surveillance technology, specifically the policies governing the use of facial recognition technology.**

In addition to enhanced reporting requirements, city council should pass legislation that codifies industry standards in the use of surveillance tools. As the OIG reports reveal, the NYPD's use of these tools lack the disciplined protocol employed by many other law enforcement agencies throughout the country.[8]

The lack of uniform, thoroughly considered policy is alarming for any new technology, but especially so in the context of facial recognition systems. As noted at the outset, the November 2022 OIG report revealed startlingly unprofessional practices surrounding the use of facial technology.[9] The NYPD's carelessness is especially disturbing given these tools' widely known risks of misidentification and wrongful convictions, particularly among women and non-white men.[10]

For example, one study conducted by MIT researchers found significant racial and gender biases embedded within facial recognition algorithms.[11] Their findings revealed that these systems

---

[7] Strauber, Jocelyn. "DOI's Office of the Inspector General for the New York City Police Department Issues Report Assessing NYPD's Compliance with the Public Oversight of Surveillance Technology Act." *The City of New York Department of Investigation*, Dec. 2024, www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf

[8] Strauber, Jocelyn, and Jeanene Barrett. "Assessment of NYPD's Response to the Post Act." *New York City Department of Investigation Office of the Inspector General for the NYPD (OIG-NYPD)*, 2022, www.nyc.gov/assets/doi/reports/pdf/2022/POSTActReport_Final_11032022.pdf

[9] (Strauber and Barrett, Section 1)

[10] Harwell, Drew. "Facial-Recognition Systems Misidentified People of Color More Often than White People, According to a Federal Study - the Washington Post." *The Washington Post*, 19 Dec. 2019, www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/
Swarns, Christina. "When Artificial Intelligence Gets It Wrong." *The Innocence Project*, 19 Sept. 2023,https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/#:~:text=More%20disturbingly%2C%20facial%20recognition%20software,be%20misidentified%20than%20white%20people; https://www.amnesty.ca/features/racial-bias-in-facial-recognition-algorithms/ .

[11] Buolamwini, Joy, and Timnit Gebru. "Intersectional Accuracy Disparities in Commercial Gender Classification." *Gender Shades*, 2018, proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

perform significantly better on male faces than female faces, with 95.9% of misgendered individuals being women.[12] Even more troubling, the study found that facial recognition tools are far more accurate for individuals with lighter skin, with leading companies exhibiting a 35% higher error rate for darker-skinned individuals.[13] This research challenges the false notion that automated systems are inherently neutral; instead, they reflect the biases of those who design and deploy them. Given these risks, the need for transparency, accountability, and strict oversight in the NYPD's use of facial recognition technology is both urgent and essential to prevent wrongful convictions and civil rights violations.

Therefore, **NYCDS supports** Int 0233-2024, a bill sponsored by Council Member Hudson which would require the NYPD to establish careful parameters governing its use of facial recognition technology and require OIG to perform biannual audits specifically reporting on the use of this technology. In addition, we urge the City Council to go further and also require that the NYPD conduct regular audits of its facial recognition tools to reveal implicit racial bias.

## 5. Conclusion

Without question, the POST Act brought some measure of oversight to the vast surveillance systems operated by the NYPD. The POST Act also provided public defenders an opportunity to review and analyze the technology and devices NYPD deploys in its day-to-day operations, so that we can better understand the new generation of evidence being used against our clients. We are grateful to the City Council for passing this landmark legislation to lay the groundwork for the important oversight and accountability that our city so badly needs.

But we now know that the POST Act did not go far enough, and that the NYPD cannot be trusted to police itself. The POST Act must be modified to provide more detailed reporting on the NYPD's surveillance operations, and impose industry-standard requirements on all extant technologies but especially on the Department's use of facial recognition technology.

As Mr. Ingram's 2020 arrest demonstrated in starkly dramatic terms, the NYPD's use of surveillance tools can very easily go horribly awry. We implore our elected leaders to acknowledge the grave potential for abuse, and take bold measures to rein in the NYPD's nearly unchecked and rapidly expanding use of surveillance technology in our city.

[12] (Buolamwini and Gebru 11)
[13] (Buolamwini and Gebru 8)

Perlmutter
Center for Legal Justice
at Cardozo Law

SEEKING JUSTICE FOR THE UNJUSTLY INCARCERATED

Joint Hearing on Oversight - Examining NYPD's Implementation of the POST Act
Committee on Public Safety and the Committee on Oversight and Investigations
February 19, 2025
TESTIMONY OF BENJAMIN BURGER
*Senior Staff Attorney, Perlmutter Center for Legal Justice at Cardozo Law*

Public Safety Committee Chair Salaam and Oversight and Investigations Committee Chair Brewer, thank you for opportunity to submit this testimony in support of Int 0168-2024 in relation to the department of investigation's oversight of the police department use of surveillance technology and Int 0480-2024 in relation to police department transparency in the use of surveillance technology.

My name is Benjamin Burger, and I am a Senior Staff Attorney at the Perlmutter Center for Legal Justice at Cardozo Law (PCLJ). PCLJ seeks justice for individuals pursuing claims of innocence and those incarcerated with excessive sentences through parole work and clemency requests. PCLJ hosts the Freedom Clinic which trains law students in the proper use of scientific evidence, focuses on how its misuse contributed to wrongful convictions, and integrates this knowledge into real casework. We also train attorneys on the underlying scientific issues in forensic science to support more robust litigation in our Forensic Science Education Program. Our multifaceted center was established through a generous donation from the Laura and Isaac Perlmutter Foundation whose philanthropy is focused on one clear and powerful goal: helping others.

Prior to joining PCLJ, I was a Staff Attorney at the Legal Aid Society for 17 years. I began my career as a public defender in the Bronx. Later, I joined the Legal Aid Society's Digital Forensics Unit, which litigates surveillance and technology issues in state courts. Int 0168-2024 and Int 0480-2024 would strengthen the Public Oversight of Surveillance Technology (POST) Act and lead to greater transparency of the powerful surveillance tools that are used by the New York City Police Department (NYPD).

On behalf of the Legal Aid Society, in October 2020, I filed a Freedom of Information Law (FOIL) request with the NYPD requesting contracts approved under the Special Expenses (SPEX) program. The SPEX program was an agreement entered into by various city agencies, including the Mayor's Office, Comptroller, and the NYPD. It allowed the NYPD to bypass the normal procurement process when purchasing surveillance technology like facial recognition software, cellphone tracking tools, and predictive policing programs. The program existed from 2007 to 2020. After the City Council passed the POST Act, Comptroller Scott Stringer withdrew from the SPEX agreement, which effectively ended the program.

Despite the NYPD denying my FOIL request and a subsequent administrative appeal, in October 2023, Supreme Court Justice Lyle E. Frank granted an Article 78 petition ordering the NYPD to provide contracts approved under the SPEX program to the Legal Aid Society.[1] Recently, the Appellate Division of the First Department upheld this decision, holding that it would not be unduly burdensome for the NYPD to comply with the FOIL statute and release the records.[2] As a result of these decisions, the public, taxpayers, and this council will be able to see how the NYPD spent $3 billion on surveillance technology.[3]

The POST Act played a substantial role in the Appellate Division's decision requiring a release of the records. However, as detailed in the reports issued by the Department of Investigation's (DOI) Office of the Inspector General for the New York City Police Department (OIG-NYPD), the NYPD has continued to "group" surveillance technologies under pre-existing Impact and Use Policies (IUP) or failed to include all the information required by the POST Act in the IUPs.

Based on my experience litigating for the release of the SPEX program contracts, despite the POST Act, New Yorkers still do not have a full picture of the NYPD's surveillance and technology capabilities. The POST Act strikes a careful balance in allowing the NYPD to deploy surveillance technology as part of its law enforcement mission, while also maintaining public oversight over powerful tools that have the potential for catastrophic abuse.

Passing the current legislation before the Council would accomplish two goals. First, it would codify the recommendations made by the OIG-NYPD in their two annual reports. This would clarify the NYPD's responsibilities under the POST Act, increase transparency, and reduce any ambiguity in the law. This is a positive result for both law enforcement and the public. Second, it would reaffirm this Council's belief that the NYPD must strike the appropriate balance between transparency and surveillance. It would send an important message to all city agencies that when powerful surveillance technologies are implemented bylaw enforcement, that law enforcement must acknowledge their responsibility to be transparent with the public, taxpayers, and the Council. I genuinely believe that the NYPD has tried to comply with the POST Act. However, by passing these bills, it would send an unambiguous message that when it comes to surveillance technology, the NYPD has the responsibility to meet the highest standards of transparency and openness.

Thank you for the opportunity to be heard on this important matter.

---

[1] *See The Legal Aid Soc. v. Records Access Officer*, No. 156967/2021, 2023 WL 7089676, at *1 (N.Y. Sup. Ct. Oct. 26, 2023).
[2] *See Legal Aid Soc'y v. Recs. Access Officer*, No. 156967/21, 2025 WL 409114, at *1 (N.Y. App. Div. Feb. 6, 2025).
[3] *See S.T.O.P., Legal Aid Society Reveal Nearly $3 Billion In Secret NYPD Surveillance Contracts*, available at https://www.stopspying.org/latest-news/2022/11/14/stop-legal-aid-society-reveal-nearly-3-billion-in-secret-nypd-surveillance-contracts (last accessed February 13, 2025).



**Joint Testimony by**

**Surveillance Resistance Lab and**

**the Street Vendor Project**

New York City Hearing with the Committee on Technology Committee on Public Safety and the Committee on Oversight and Investigations on Oversight and Legislation: Examining NYPD's Implementation of the POST Act

February 19, 2025 at 10 am at

Committee Room - City Hall

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

Written testimony submitted via New York City Council portal, February 21, 2025

**Thank you to the Chairs, and members of all the committees, for holding this public hearing** and allowing us the opportunity to share our concerns about the NYPD's widespread use of technologies, data and personnel through other city agencies to surveil New Yorkers and attempt to avoid mandatory reporting requirements. I present this testimony today jointly on behalf of both the Surveillance Resistance Lab and the Street Vendor Project.

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.

The Street Vendor Project is a membership-based organization of over 3,000 street vendors working together to create a movement of vendors for permanent change across the city.

**We testify jointly today to bring attention to technologies used by the NYPD to surveil New Yorkers through coordination with other agencies – with a specific focus on how this impacts street vendors, many of whom are immigrants.**

We testify today to emphasize how street vendor policing through cross agency data and personnel sharing raises questions about additional unreported surveillance technologies used by the NYPD, unlawful profiling and what is now obviously dangerous mapping of immigrant communities.

This echoes what many Black and Latino New Yorkers have experienced from decades of intense broken windows policing and stop and frisk. What lurked beneath the surface of the "quality of life" policing goals was also data collection and community mapping by police. A similar iceberg lurks beneath the surface today with street vendors policing and mapping immigrant communities.

**In spite of the reporting required by the POST Act, the NYPD fails to report the many mechanisms through which it surveils New Yorkers by collecting information about them. This is especially true of the data collected on low income or disabled New Yorkers from immigrant, Black, and other communities of color who rely on city services as well as those who survive financially as street vendors.**

We ask that the City Council mandate the NYPD to report the full breadth of technologies NYPD uses to surveil, including technologies and data it has access to through other agencies plus city and state task forces, so that they may also be publicly debated.

While the POST Act defines surveillance technology as technology "that is operated by or at the direction of the department," the NYPD narrowly interprets this to exclude the increasing number of data sharing technologies used to gather information from other city agencies involved in policing and surveilling New Yorkers—none of these systems are reported on by the NYPD.

It is increasingly critical that the NYPD include the data sharing technologies the agency relies on as it escalates cross-agency efforts to utilize peace officers operating within traditionally civilian agency to enforce city rules and regulations. For example, the policing arms of the Department of Sanitation and Parks Department are increasingly utilized in operations that target street vendors across the City.

Today we call attention to the data sharing practices across multiple agencies including the NYPD, the Department of Sanitation, the Department of Health and Mental Hygiene, the Parks Department, and more.

As we heard during the hearing, through task force MOUs, data becomes accessible to all members of the task force. **While the NYPD may not collect data for federal civil immigration policing, the Community Link task force that includes the NYPD is absolutely targeting immigrants for data collection through street vendor policing.**

As an example, the NYPD's Operation Restore Roosevelt was launched in October 2024 through the Mayor's Community Link initiative. Community Link is described on its website as "A Multi Agency Response for Quality-Of-Life Issues." It promises to "to help address complex and often chronic community complaints that require a multi-agency response." And yet in January 2025, when the Mayor announced the results of having 20 city agencies working together, the outcomes were limited to arrests, summonses, and seizure of property.

In other words, Operation Restore Roosevelt relied on resources from 20 various city agencies to carry out a policing project. It is policing but with a different name. Rather than addressing the causes of the "quality of life" conditions in their complexity for all, as promised, Operation Restore Roosevelt proved to only produce a harmful police response.

Cross agency collaborations like Community Link allow the NYPD to access a vast array of technologies to surveil New Yorkers and yet they fail to identify them in POST Act reporting. On the Lab's website you can find more information about the Digital Cop City iceberg–it maps how digital data collection and sharing infrastructure hidden beneath the surface expands the power of the NYPD and corporations in the city.

**Beyond data sharing, it also allows the NYPD to control a large number of peace officers who are not beholden to NYPD accountability and oversight mechanisms.** Citywide, there are approximately 250 Parks Enforcement Police (PEP) and 40 Department of Sanitation Police (DSNYP) operating as Peace Officers, both with a duty to 'enforce street vending.' In 2024, the NYPD Deputy Inspector Timothy Wilson was assigned as "Chief of Enforcement" at Parks to lead the PEP—part of a larger initiative to place NYPD officials into local government agencies.

Yet there are little to no accountability measures for the Parks Enforcement Police and Department of Sanitation Police. The Civilian Complaints Review Board's purview extends only to the NYPD—in order to report a complaint against PEP, one must submit a complaint to the NYC Parks Department directly, and similarly complaints against the DSNY Police must be made to the Department of Sanitation Inspector General.

**Not surprisingly, Operation Restore Roosevelt has not improved the quality of life equitably for the diverse communities that call Jackson Heights and Corona home.** Laura Torlaschi, a Queens-based writer and sex work advocate for DecrimNY, punctured the PR campaign of Community Link as a cross-agency effort by asking in an op-ed: "what happens after the cops?" So far, beyond policing, the community has not seen anything.

Contrary to action that would actually distribute supportive social services to residents of Jackson Heights, other members of City Council have called for the creation of a portal through the Office of Street Vendor Enforcement (OSVE) "that would allow all agencies enforcing street vending laws and regulations to share enforcement-related information." These data-sharing technologies must also be included in POST Act reporting because they too are surveillance technologies used by the NYPD. This becomes all the more critical if the City capitulates to federal immigration policing.

**The purpose and extent of data sharing between police and all other agencies through initiatives like Community Link but also through new technologies—such as those adopted by New York public schools, , benefits portals like MyCity, the sanitation Trash Dash, and citywide data sharing systems like Worker Connect—should all be publicly reported and debated.**

THE LEGAL AID SOCIETY

Justice in Every Borough.

# TESTIMONY

The Council of the City of New York
Committee on Technology, Committee on Public Safety, and the
Committee on Oversight and Investigations

An oversight hearing examining the New York City Police Department's implementation of the Public Oversight of Surveillance Technology (POST) Act

February 19, 2025

The Legal Aid Society
Criminal Defense Practice
49 Thomas Street
New York, NY 10013

By: Jerome D. Greco
Digital Forensics Unit
Digital Forensics Director
(212) 298-3075
JGreco@legal-aid.org

## Contents

Good morning. I am Jerome Greco, the Director of The Legal Aid Society's Digital Forensics Unit, a specialized unit providing support for digital evidence and electronic surveillance issues for The Legal Aid Society's attorneys and investigators, in all five boroughs. I thank these Committees for the opportunity to provide testimony on the New York City Police Department's implementation of the Public Oversight of Surveillance Technology (POST) Act. To avoid being overly repetitious, I incorporate by reference my testimony from the December 15, 2023 oversight hearing[1] here and will attempt to mostly address updates and issues that have arisen since then.

## I. ORGANIZATIONAL INFORMATION

Since 1876, The Legal Aid Society has provided free legal services to New York City residents who are unable to afford private counsel. Annually, through our criminal, civil and juvenile offices, our staff handles over 180,000 matters for low-income families and individuals. By contract with the city, the Society serves as the primary defender of indigent people prosecuted in the state court system.

In 2013, The Legal Aid Society created the Digital Forensics Unit to serve and support Legal Aid attorneys and investigators in our criminal defense offices. Since that time, we have expanded to two digital forensics facilities, three analysts, two senior analysts, six staff attorneys, one paralegal, and one director. Members of the Unit are trained in various forms of digital forensics and have encountered multiple different types of electronic surveillance used by law enforcement.

[1] Oversight Hearing Testimony, Dec. 15, 2023, available at https://legistar.council.nyc.gov/View.ashx?M=F&ID=12694289&GUID=69AB5205-826E-4D47-9557-0915D8574EFF [last accessed Feb. 17, 2025].

## II. BACKGROUND ON THE POST ACT

The Public Oversight of Surveillance Technology (POST) Act was originally introduced by Council Member Daniel Garodnick in 2017 but was never brought to a vote. It was reintroduced with the same language in 2018 by Council Member Vanessa Gibson, and finally brought to a vote in 2020. The City Council overwhelmingly passed the POST Act 44 to 6, with minimal changes to the original language. On July 15, 2020, it was signed into law by Mayor Bill de Blasio and enacted as Local Law 65.

The POST Act, at its core, required "the reporting and evaluation of surveillance technologies used by the NYPD."[2] It further directed that:

> The Department will be required to issue a surveillance impact and use policy about these technologies. The policy would include information on surveillance technologies such as the description and capabilities, rules, processes and guidelines, and any safeguards and security measures designed to protect the information collected. Upon publication of the draft surveillance impact and use policy, the public shall have a period of time to submit comments. The commissioner of the department shall consider the comments and provide the final version of the surveillance impact and use policy to the Council, the Mayor and post to the Department's website. The inspector general for the NYPD shall audit the surveillance impact and use policy to ensure compliance with its terms.[3]

Despite the minimal transparency the POST Act required of the NYPD, they have failed to follow its mandates. They have resisted following the letter and the spirit of the law and have sought to exploit any perceived vagueness or flaw in the law's language.

---

[2] Summary of Int. 0487-2018, available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0 [last accessed Feb. 17, 2025].

[3] *Id*.

## III. THE NYPD SPECIAL EXPENSES ("SPEX") BUDGET FOIL LITIGATION

As I previously testified to in the December 15, 2023 oversight hearing, for over a decade, the NYPD was permitted to conceal its purchase of surveillance technologies – contracts that were otherwise subject to public accessibility and disclosure. Through an agreement with the Law Department, the Mayor's Office of Contract Services, Department of Investigation, Office of Management and Budget, and the City Comptroller's Office, the NYPD hid these contracts and expenditures under the Special Expense ("SPEX") Budget.

After the POST Act was enacted into law in the summer of 2020, the City Comptroller's Office withdrew from the SPEX budget MOU and Amendment.[4] In a letter to NYPD Commissioner Dermot Shea, Comptroller Scott M. Stringer cited the POST Act as the reason for his office withdrawing from the agreement.[5] The passage of the POST Act helped end a thirteen-year agreement between multiple city agencies that allowed the NYPD to avoid any public scrutiny for how it spent taxpayer money on electronic surveillance tools.

Despite the POST Act and the dissolution of the original agreements, the NYPD has fought against the release of the SPEX budget contracts and related records for over four years. In 2020, The Legal Aid Society sent a FOIL request to the NYPD for unredacted copies of the contracts and related records that fell under the SPEX budget. The NYPD denied the request in

[4] Rocco Parascandola, *Comptroller Stringer tells NYPD surveillance technology expenses can't be kept secret*, New York Daily News, July 31, 2020, available at https://www.nydailynews.com/2020/07/31/comptroller-stringer-tells-nypd-surveillance-technology-expenses-cant-be-kept-secret/ [last accessed Feb. 17, 2025].

[5] *NYC Comptroller Letter to NYPD Commissioner Shea Terminating Special Expense Budget Memorandum of Understanding*, July 30, 2020, available at https://archive.org/details/nyc-comptroller-letter-to-nypd-comissioner-shea-terminating-special-expense-budg [last accessed Feb. 17, 2025].

full initially and on administrative appeal. As a result, The Legal Aid Society filed an Article 78 in New York County Supreme Court to force the NYPD to comply with the FOIL request.[6]

A hearing was held on the matter on July 10, 2023, in front of the Honorable Lyle E. Frank. On October 27, 2023, the court ruled in favor of The Legal Aid Society, requiring the NYPD to provide the requested records.[7] Soon thereafter, the NYPD filed an appeal to the First Department, and the trial court's decision and order was put on hold, pending the outcome of the appeal.

On appeal, The Legal Aid Society and Orrick, Herrington & Sutcliffe LLP, prevailed. Earlier this month, the First Department affirmed the lower court's ruling, requiring the NYPD to provide the SPEX budget surveillance related contracts.[8] A notice of entry has been filed, and we are now waiting to see if the NYPD will attempt to appeal further to the Court of Appeals.

In the appellate court's decision, it partially relied on the passing of the POST Act and the termination of the original SPEX budget agreement to adopt Legal Aid's arguments and to reject the NYPD's claims:

> Crucially, the NYPD made no effort to contend with the seismic shift caused by the POST Act. Murtagh made only passing mention of the public disclosures required by the POST Act and made no attempt to explain how those disclosures might affect the NYPD's claim of exemption. Because of the POST Act, the contracts in question no longer describe technologies hidden from the public. These technologies have been described by the NYPD itself in its published Final Surveillance and Use Policy. Thus, the NYPD failed to demonstrate, or even approximate, the portion of the documents that would fall within the exemption for nonroutine criminal investigative techniques or procedures. (Public Officers Law § 87[2][e][iv]).[9]

---

[6] *Legal Aid Society v. Records Access Officer*, Index No. 156967/2021 (N.Y. Co. Sup. Ct.).

[7] *Legal Aid Society v. Records Access Officer*, 2023 WL 7089676 (N.Y. Co. Sup. Ct. 2023).

[8] *Legal Aid Society v. Records Access Officer*, 2025 NY Slip Op 00723 (1st Dept. 2025).

[9] *Id*. at *4.

Overall, the POST Act has been a success for transparency, but it also falls short in many ways. The City Council now has the opportunity to fix some of these flaws. It should not take over four years of litigation just to get the NYPD to provide basic contractual information regarding the surveillance tools they have purchased. The Council has the ability to patch any claimed holes in the POST Act and strengthen its main purpose, to provide transparency for advocates and the general public about how the NYPD purchases and uses electronic surveillance tools.

## IV. POST ACT FAILURES

Many of the NYPD's failures to comply with the POST Act have been documented in The Legal Aid Society's previous testimonies, comments to draft policies, complaints made to the Department of Investigation, and in the DOI's annual reports. Here, I will focus on three technologies: unmanned aircraft systems (drones), facial recognition technology, and the Evolv weapons detection system. Since The Legal Aid Society and the DOI have extensively described the many problems with the NYPD's use of drones and facial recognition technology, I will only address the issues that have not previously been covered or have not received sufficient attention.

### A. Unmanned Aircraft Systems (Drones)

The most recent report from the DOI NYPD Inspector General on the NYPD's compliance with the POST Act already covered many of problems associated with the NYPD's use of drones, including not updating the Impact and Use Policy[10] and Patrol Guide to address their current use and failing to provide complete deployment reports to the DOI.[11]

[10] NYPD Unmanned Aircraft Systems: Impact and Use Policy, Sept. 22, 2023, available at https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/Unmanned_Aircraft_Systems_UAS_NYPDIUP_Addendum_9.22.23.pdf [last accessed Feb. 17, 2025].

[11] NYC Department of Investigation: Office of the Inspector General for the NYPD, An Assessment of NYPD's Compliance with the POST Act, Dec. 2024, available at

An additional issue is that the NYPD is not completing required documentation or retaining required records and data when a drone is used pursuant to the Drone First Responder (DFR) program. The DOI report discussed that drones flown pursuant to the DFR were often not complying with the IUP or the procedures laid out in the NYPD Patrol Guide. We can now confirm that in some cases the prosecutors have been unable to provide deployment reports because NYPD personnel were not completing them, video footage because the NYPD was allowing it to be overwritten without first preserving a copy, or metadata, which was also being overwritten and not preserved. It appears that the DFR program not only violated the NYPD's own procedures, but also violated New York State's discovery law.

B. Facial Recognition Technology

In addition to the many problems with police use of facial recognition technology,[12] there have been three NYPD specific issues that have mostly been unaddressed: providing potential facial recognition matches to other agencies outside of New York City, using potential facial recognition matches prepared by an agency other than the NYPD, and using a potential facial recognition match to perform unduly prejudicial identifications procedures with another officer as the identifier.

There is not enough detail about how the NYPD permits the use of its facial recognition technology to help investigations conducted by agencies outside of New York City. The Legal Aid Society is aware of it happening on multiple occasions, but the most public example

https://www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf [last accessed Feb. 17, 2025].

[12] Douglas MacMillan, David Ovalle & Aaron Schaffer, *Arrested by AI: Police ignore standards after facial recognition matches*, The Washington Post, Jan. 13, 2025, available at https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/ [last accessed Feb. 17, 2025].

occurred in a New Jersey state case. In *State v. Arteaga*,[13] after the New Jersey Regional Operations Intelligence Center was unable to generate a possible facial recognition match of a suspect captured on surveillance video, the NYPD Facial Identification Section developed a possible match using the NYPD's facial recognition technology. The Facial Recognition Impact and Use Policy[14] appears to allow for the NYPD to provide assistance to outside law enforcement agencies, but it is unclear how often this is done, the procedures in place to ensure that the other agencies comply with the NYPD rules or any laws, how the NYPD determines which agency to help or not, and how often the NYPD has provided this service to other law enforcement agencies.

Similarly, the NYPD appears to use possible facial recognition matches provided by other agencies as part of NYPD investigations. In at least one case known to The Legal Aid Society, the New York City Fire Department supplied a potential facial recognition match to the NYPD, which had been obtained through the use of Clearview AI. It is currently unknown how or why the FDNY became involved. Similarly, it is unclear what the NYPD's policies are about using facial recognition matches that are performed by an external agency. In this specific case though, it appears that it violated the NYPD's IUP because "[t]he use of facial recognition technology that compares probe images against images outside the photo repository is prohibited unless approval is granted for such analysis in a specific case for an articulable reason by the Chief of Department, Chief of Detectives, or Deputy Commissioner, Intelligence and Counterterrorism." Clearview AI compares probe images with images scraped from the internet

[13] 476 N.J. Super. 36 (N.J. Super. Ct. App. Div. 2023).

[14] NYPD Facial Recognition: Impact and Use Policy, Nov. 24, 2023, available at https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/facial-recognition-nypd-impact-and-use-policy_11.24.23.pdf [last accessed Feb. 17, 2025].

and social media, which are outside of the NYPD's photo repository, but this did not prevent the NYPD from using the result obtained from the FDNY, nor does it appear that any of the individuals authorized to grant an exception did so.

When there is no eye witness to an alleged crime, the eye witness is unavailable, or the eye witness does not identify the person selected via facial recognition as the perpetrator in a photo array, the NYPD will often depend on unreliable identifications from officers that are otherwise unconnected to the case in order to generate alleged probable cause. After receiving the possible facial recognition match, the case detective will look in the NYPD's databases for an officer that has had a previous contact with the suspect identified by facial recognition, regardless of how limited that contact may have been. This officer will have no connection with the ongoing investigation and often works in a different unit or precinct. The officer will receive an email from the case detective with either the original video attached or a still from the video, requesting if the officer can identify the person depicted. Since the officer has no connection to the case and is being specifically and individually contacted about the person's identity, it is clear that he knows that the case detective already believes the officer has had contact with the depicted person. Then the officer thinks of who he has prior contact with, and sometimes even reviews his own case files, to determine who most looks like the person depicted. The officer will then let the case detective know that the officer knows the depicted person and provide a name. This is not a true identification procedure because it already hints to the officer who the person depicted may be, and the officer is selecting who he has had contact with that most looks like the person depicted, rather than identifying that person because he actually knows it is them. The NYPD considers this enough to establish probable cause and make an arrest, even though it is a clearly contrived procedure that intentionally lends itself to bias and false identifications.

C. Evolv Weapons Detection System

On March 28, 2024, the NYPD posted a draft Electromagnetic Weapons Detection System Impact and Use Policy,[15] which was deficient in multiple ways. The Legal Aid Society submitted a letter pointing out many of the problems with the IUP during the public comment period.[16] Under the timelines set out by the POST Act, after the required 45-day comment period concluded, the NYPD had another 45 days to publish its finalized policy. However, almost a month after the deadline for the final policy had passed it still had not been issued. This failure did not deter the mayor from announcing that the NYPD was starting a 30-day trial of an alleged weapons detection system from Evolv Technology. It was only after The Legal Aid Society publicly rebuked the NYPD for both its violation of the POST Act, and its bad judgment in moving forward with testing the detectors,[17] that the final policy was posted on July 25, 2024.[18]

Besides violating the timing of the posting of the impact and use policy, the final policy failed to address the many issues that existed in the draft version, including the mounting criticism that Evolv's product is not effective and prone to false alerts. There are a litany of valid criticisms of this weapons detection system and the NYPD's attempted use of them in the

[15] NYPD Electromagnetic Weapons Detection System: Draft Impact and Use Policy for Public Comment, Mar. 28, 2024, available at https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/electromagnetic-weapons-detection_iup_3.28.24_draftforcomment.pdf [last accessed Feb. 17, 2025].

[16] The Legal Aid Society, *Comments on the NYPD March 28, 2024 Draft Impact and Use Policy for Electromagnetic Weapons Detection System*, May 9, 2024, available at https://legalaidnyc.org/wp-content/uploads/2024/05/Legal-Aid-Society-Comments-to-Electromagnetic-Weapons-IUP.pdf [last accessed Feb. 17, 2025].

[17] Chris Sommerfeldt, *NYPD planned launch of weapons detectors in MTA subways violates privacy laws, advocates say*, New York Daily News, July 24, 2024, available at https://www.nydailynews.com/2024/07/24/nypd-launch-of-weapons-detectors-in-mta-sbways-premature-advocates-say-evolv/ [last accessed Feb. 17, 2025].

[18] NYPD Electromagnetic Weapons Detection System: Impact and Use Policy, July 25, 2024, available at https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/electromagnetic-weapons-detection-iup_posted_7.25.24.pdf [last accessed Feb. 17, 2025].

subways, most of which were included in our comments to the draft policy. Examples of issues with Evolv and its product that the NYPD didn't address include: their own CEO stating that the subway was a "not a good use case,"[19] some of its own shareholders suing the company and alleging that the system "does not reliably detect knives or guns,"[20] being investigated by multiple federal government agencies,[21] and that the electromagnetic radiation emitted from the Evolv system may interfere with implanted medical devices.[22] Furthermore, and potentially most relevant to the system's lack of effectiveness, during a 7-month pilot at Jacobi Medical Center, approximately 43,800 of 50,000 alarms from the Evolv detectors – nearly 85% – were false positives.[23]

The results of the NYPD Evolv pilot confirmed that many of the concerns were justified. During the thirty-day trial across twenty subway stations, the NYPD performed 2,749 total

[19] Michael Gartland & Evan Simko-Bednarski, *CEO of weapon scanner company showcased by NYC Mayor Adams: Subways not a "good use-case,"* New York Daily News, Mar. 29, 2024, available at https://www.nydailynews.com/2024/03/29/weapon-scanner-company-showcased-by-nyc-mayor-adams-subways-not-a-good-use-case-underground/ [last accessed Feb. 17, 2025].

[20] Jason Koebler, *Shareholders Sue AI Weapon-Detecting Company, Allege It "Does Not Reliably Detect Knives or Guns,"* 404 Media, Mar. 29, 2024, available at https://www.404media.co/shareholders-sue-evolv-ai-weapon-detecting-company-because-it-fails-to-detect-weapons/ [last accessed Feb. 17, 2025].

[21] Todd Shields & Leah Nylen, *FTC Probes Evolv Security Over AI Weapons Screening Claims*, Bloomberg, Oct. 13, 2023, available at https://www.bloomberg.com/news/articles/2023-10-13/ftc-probes-evolv-security-over-ai-weapons-screening-claims [last accessed Feb. 17, 2025] and Evolv Investor Relations, *Evolv Technology Provides Regulatory Update*, Press Release, Feb. 19, 2024, available at https://ir.evolvtechnology.com/news/press-releases/detail/177/evolv-technology-provides-regulatory-update [last accessed Feb. 17, 2025].

[22] Andy Sheehan, *Woman says her implanted medical device stopped working after going through PNC Park security system*, CBS News, Sept. 12, 2023, available at https://www.cbsnews.com/pittsburgh/news/implanted-medical-device-qustions-evolv-security-system/ [last accessed Feb. 17, 2025].

[23] Felipe De La Hoz, *NYC Has Tried AL Weapons Scanners Before. The Result: Tons of False Positives*, Hell Gate, Apr. 2, 2024, available at https://hellgatenyc.com/nyc-ai-weapons-scanners-pilot-false-positives/ [last accessed Feb. 17, 2025].

scans.[24] No firearms were recovered, twelve knives were recovered, and there were 118 false positives.[25] It is unclear whether any of the twelve recovered knives were unlawful to possess or resulted in any arrests. Regardless, the criticisms and comments that the NYPD ignored and refused to address were proven correct. Despite the trial ending and the terrible results, the IUP is still posted without any changes.

## V. LEGISLATION TO UPDATE THE POST ACT

There are three bills that have been introduced to fix some of the perceived and actual flaws of the POST Act. Council Member Amada Farías has introduced Int. 0168-2024:

> This legislation would add new provisions to the law which would require that the NYPD, upon request, provide the Department of Investigation (DOI) with an itemized list of all surveillance technologies currently used by the Department, and provide information on all data access and retention policies for data collected by such technologies. In addition, the legislation requires that the NYPD provide DOI with quarterly updates on all newly acquired or discontinued surveillance technologies and updates to any data access and retention policies established in recently executed contracts for surveillance technologies.[26]

Council Member Crystal Hudson has introduced Int. 0233-2024:

> This legislation would require the New York City Police Department (NYPD) to publish on its website a written policy that establishes procedures and regulations for the Department's use of facial recognition technologies. The legislation would also require that the NYPD conduct biannual audits of the Department's use of facial recognition technology, share the findings of such audits

[24] Annie McDonough, *The results are in! Evolv gun scanners recover zero guns in subways*, City & State New York, Oct. 24, 2024, available at https://www.cityandstateny.com/politics/2024/10/results-are-evolv-gun-scanners-recover-zero-guns-subways/400522/ [last accessed Feb. 17, 2025].

[25] *Id*.

[26] Summary of Int. 0168-2024, available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6557506&GUID=5821E50A-2DB7-49F9-B89A-0701A980CB79 [last accessed Feb. 17, 2025].

> with the Department of Investigation, and post such findings on the Department's website.[27]

Council Member Julie Won has introduced Int. 0480-2024:

> This legislation would clarify language in existing law to ensure increased transparency in NYPD's required "Impact and Use," specifically requiring: (1) that NYPD publishes Impact and Use policies for each individual surveillance technology used by the Department; (2) that such Impact and Use policies fully identifies each external entity by name that receives data gathered from such technology; (3) that such Impact and Use policies report on the safeguards in place to prevent dissemination of surveillance data; and (4) that such Impact and Use policies adequately disclose evaluation of potential disparate impacts on protected groups arising from the NYPD's use such technologies.[28]

Int. 0168-2024 will allow for the Department of Investigation to provide better informed oversight over the NYPD, in the way the POST Act originally intended, by requiring the NYPD to turn over information that is clearly relevant to the DOI's responsibilities. Similarly, Int. 0480-2024 will require the NYPD to provide more information than it currently does by closing alleged loopholes and clarifying language that they NYPD had chosen to interpret in the way that provided less transparency and accountability. Essentially, it will restore the original intent and goals of the POST Act.

Many of the NYPD's electronic surveillance tools should not be used at all because of their ability to cause harm, the disparate impact of that harm on Black and brown communities, the difficulty addressing the harms caused by these technologies in courts, and their pervasiveness. However, all three bills are admirable in their attempts to prevent the NYPD from

[27] Summary of Int. 0233-2024, available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6557579&GUID=CBBA0BE3-696A-4A94-A212-46163F1FED29 [last accessed Feb. 17, 2025].

[28] Summary of Int. 0480-2024, available at https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6558150&GUID=93128EDA-AF40-4B9E-9E77-6F8696E2F718 [last accessed Feb. 17, 2025].

continuing their abuse of surveillance technology and hiding behind claimed loopholes in the original version of the POST Act. Transparency is a necessary step towards accountability, and the more information that is available about the NYPD's surveillance arsenal, the better defense attorneys can challenge their use and the better they can inform their clients about the legal and factual issues in their cases.

## VI. CONCLUSION

The passing of the POST Act had laudable intentions, but the NYPD has chosen to "comply" in ways that attempt to defeat the law's purpose. While many of the NYPD's electronic surveillance tools should be banned, updating the POST Act to achieve the transparency intended by the original bill would be a step in the right direction. The Legal Aid Society encourages the City Council to enact into law the changes we have endorsed here.

of Law

NYU School

40 Washington Square South
New York, NY 10012

E: tech@policingproject.org
W: policingproject.org

**NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY JOINTLY WITH COMMITTEE ON PUBLIC SAFETY AND COMMITTEE ON OVERSIGHT AND INVESTIGATIONS**

HEARING:

Public Hearing on Int. 0168-2024, Int. 0233-2024, Int. 0480-2024, Feb. 19, 2025

DATE OF TESTIMONY:

Feb. 19, 2025

TESTIMONY OF THE POLICING PROJECT AT NYU SCHOOL OF LAW IN SUPPORT OF INT. 0168-2024, INT. 0233-2024, INT. 0480-2024

Dear Chairs Gutiérrez, Salaam, and Brewer and Committee Members:

Thank you for calling this important public hearing to discuss ways to improve NYPD's implementation of the POST Act (the "Act"). In this testimony, we want to make three points:

- First, we agree with civil society advocates and NYPD's own Inspector General that NYPD's incomplete and inadequate policy disclosures flout the intent of the POST Act and violate the public's interest in transparency.
- Second, we want to express support for the three bills offered today that are designed to strengthen the Act's disclosure requirements.
- Finally, we urge this body to pass additional amendments that would: (1) require NYPD to develop intergovernmental data-sharing policies and (2) add transparency provisions to NYPD's facial recognition use policy.

But first, some brief background on our work. The Policing Project's mission is to partner with communities and police to promote public safety through transparency, equity, and democratic engagement. Our work is focused on ensuring democratic accountability and public participation ***on the front end.*** By this, we mean that the public should have a voice in setting transparent, ethical, and effective policing policies and practices ***before*** the police act. Although this type of accountability is common in other areas of government, it is rare in policing.

Legislation like the POST Act is essential to democratic accountability because it fosters transparency, a foundational principle to sound

governance. By requiring the NYPD to disclose publicly each surveillance technology it intends to use and to publish impact and use policies ("IUP") for those technologies, the POST Act provided a much-needed first step towards transparency and accountability. This ensures New Yorkers can meaningfully engage in public debate about how these technologies should be used.

However, despite the important goals of this law, the NYPD has consistently failed to provide the kind of meaningful transparency the Act intended to require. Now, three bills—Int. 0168, Int. 0233, and Int. 0480—before the New York City Council aim to strengthen the Act and ensure the NYPD is held accountable for its use of surveillance technologies. This slate of bills would add more stringent and specific reporting requirements to the existing obligations outlined in the Act. Accordingly, we broadly support each of these bills and their aim of ensuring meaningful transparency and accountability.

NYPD violated the intent of the Act by creating vague IUPs that defy its intended disclosure requirements. Since the passage of the POST Act, the NYPD has faced criticism not only from civil liberties advocates, but also from the Office of the Inspector General (OIG). A report from the OIG found that even though the Act requires the NYPD to report information about any data sharing with third parties in its impact and use policies, NYPD's IUPs were so "broad and general" regarding data-sharing that they "fail[] to convey to the public any specific information about the agencies that can access the relevant data." This leaves the public bereft of any information about who can access the data collected about them, and whether the recipients of such data are using it responsibly. Int. 0480 directly addresses this issue by requiring the NYPD to specifically name the entities with whom it is sharing data and specify any safeguards or restrictions imposed on each entity's use or dissemination of information collected.

The OIG also reported that the NYPD grouped distinct technologies together under the same policy—a tactic that essentially undermines the goals of transparency and limits public oversight. For example, when the NYPD acquired Digidog, a robot dog with mounted microphones and cameras, there was no individual IUP. Instead, the robot was grouped with their broader policies for "situational awareness cameras." Although the NYPD claimed it maintained an internal itemized list of surveillance technologies, the list lacked details on functionality and capabilities, making it difficult for OIG to assess compliance with the Act. This practice also enables the NYPD to bypass disclosure requirements for new technologies. As such, to the extent to which the Act is unclear, Int. 0480 requires impact and use policies for all distinct surveillance technologies in use. Additionally, Int. 0168 requires the NYPD, upon request, to provide an itemized list of all surveillance technologies in use. This list goes beyond existing POST Act mandates by requiring the NYPD not just to disclose each technology's capability, but also the types of data collected and the department unit responsible for each. It also requires the NYPD to provide a quarterly list of all newly acquired and discontinued surveillance technologies. This ensures NYPD

creates IUPs for all surveillance technologies in its control and provides sufficient information for OIG to assess NYPD's compliance with the Act.

Int. 233 would require the NYPD to publicly post written policies for its use of facial recognition technology (FRT), including, at minimum, a description of its use, restrictions on access and use by NYPD personnel, and data retention policies - adding much-needed transparency. The NYPD has continuously ignored the spirit of the law when it comes to its use of FRT. Although the NYPD is required by the Act to publish an IUP for FRT, the policy offers little substantive information about its application, data sharing practices and retention practices.

***Suggested Improvements***

These three bills are critical in codifying both the original intent of the POST Act, as well as the responsive OIG recommendations. However, we believe further refinements to Int. 0480 and Int. 0233 could enhance their impact:

Int. 0480 should require the NYPD to develop formal intergovernmental data-sharing policies that detail when data collected by surveillance technologies can be shared with other government agencies, the criteria for sharing data, the type of data shared, and with whom. Establishing these policies will foster responsible and accountable use of sensitive surveillance data by government agencies by ensuring data is only disclosed for legitimate purposes and facilitating meaningful auditing of the department's compliance with the law.

Int. 0233 rightly requires more rigorous standards for how the NYPD reports its use of FRT through published written policies. These standards can be further strengthened by requiring the NYPD policy to include: (1) disclosure to the accused for any case in which FRT was used and a criminal proceeding commenced, whether or not a suspect was identified using FRT; (2) documentation on the types of crime for which FRT was used and its outcomes, such as the resulting enforcement action or the number of times a person was wrongly identified; and (3) provisions only permitting law enforcement use of FRT systems from vendors who have demonstrated high accuracy with law enforcement's intended image quality and across demographic groups in real-world deployment contexts. These additional measures will equip criminal defendants with crucial information to mount an adequate defense, provide the public with essential information about the effects of NYPD's use of FRT, and ensure NYPD only uses FRT systems that have proven to be reliable and accurate. Accordingly, these measures will ensure that the NYPD acquires and deploys FRT in a way that is effective, accountable, and fit for community needs.

The POST Act was a necessary first step in promoting transparency, but it is clear that stronger oversight is needed to prevent the NYPD from sidestepping its obligations. These three bills represent a crucial effort to close the gaps in the law and reinforce accountability in

policing. We therefore urge the Council to pass these measures. Thank you for considering our testimony.

**From:** [redacted]
**To:** [redacted]
**Subject:** [EXTERNAL] Ref : Follow up with Testimony about POST ACT
**Date:** Sunday, February 23, 2025 2:52:23 AM
**Attachments:** Radiation Letter.docx

---

[redacted]

Dear Chair  Salaam,
Dear Chair Brewer,
Dear Chair Gutierrez
And Members of the Council
My name is Pastor Adlerette Kebreau and I thank you for the opportunity to testify on Havana Syndrome or microwave Radiation an Evil Technology that is not part of POST ACT Law 65 on February 19, 2025 along with my collaborator Michele Anne Blondmonville.
Below is an attachment of my testimony demanding that you guys follow the Colorado Law as to BAN all forms of Direct Energy Weapons Technology in NY.
Be aware that there are other witnesses cc in this conversation.

Again, thank you for your expedited collaboration on this matter.
Pastor Adlerette Kebreau

**Monday February 24, 2025**

**Save Yourself**

**Save your love Ones**

**Save your Constituents**

**Save America**

**Save our Constitution**

**"NO CORRUPTION/ COVER UP WILL EVER STOP UNLESS THERE IS REAL INVESTIGATION''**

**Chair Salaam,**

**Chair Brewer,**

**Chair Gutierrez, and Members of the City Council Committees, on Public Safety, Oversight and Investigation and Technology**

**STATEMENT OF PASTOR ADLERETTE KEBREAU**

**International Ministry of Jesus Christ Heart**

**Accompanied by Michele Anne Blondmonville**

**On February 19, 2025, the Joint Committees had a hearing on Public Safety and Technology**

**The committees were focusing on POST ACT, signed into law by Mayor De Blasio and enacted as Local Law 65.**

**My Question is you aware of all the Technology on the Market?**

**Does NYPD have disclosed all the different types of Technology they have been using?**

**One of the testimonies was the UAS IUP inaccurately states that ( ALL) drone deployments are operated and supervised by TARU, when in fact multiple units within NYPD ( OPERATE) their own drone programs.**

**What are the mechanisms do you have in place to know the different types of technology that are on the market and the ones that have been used by NYPD or perhaps by Private or Non Private Agencies ?**

**As I sat through the entire hearing I have noticed that there are certain technology that are on the market, that NYPD may have used ,or other entity may use but POST ACT did not cover such technology. A dangerous technology destroying lives.**

**On May 8, 2024, the World has watched one of his kind congressional meetings held by the Committee of Homeland Security on Silent and Unseen Weapons or DIRECTED ENERGY WEAPONS.**

**Examining Foreign Havana Syndrome or Anomalous Health Incident targeting Americans in the Homeland. Over thousands of Innocent Americans, targeted Individuals were thankful for this meeting, but apparently, the committee of the Homeland Security is grossly uninformed**

**about this Covert and Unconstitutional existence of this horrible evil criminal non-touch torture of Law Abiding Citizens on the Soil of the United of America.**

**These weapons are not new in America, according to Former President His Excellency Bill Clinton in 1995 had apologized to America and particularly to the survivors and families of those unknowingly were subjects of Direct Energy Weapons or Microwave Radiation sponsored by the American Government in America see #Exhibit A.**

**In 2016, the State Dept. first reported Havana Syndrome publicly, few years later 60 Minutes had a report of US Diplomats with Havana Syndrome see Exhibit E**

**1-What are Directed Energy Weapons or Microwave Radiation – or Silent Weapons?**

**It is some type of Technology use concentrated electromagnetic energy to combat enemy forces and assets. For much more details see #Exhibit B**

**2- Since no naked eyes can see the operation of those Silent Weapons, the public including many of the mainstream media believe such weapons do not exist, don't they?**

**It was told for quite some times there was no such weapons as those silent and unseen Directed Energy Weapons. Many were even told they were crazy and some even were forced to go under evaluation, it was False. DOD Defense Secretary Dr Mark T Esper admitted in a video dated 9/16/2020 that this "Kind of Technology does exist by the US government see Exhibit C.**

**Furthermore, more evidence of such weapons are well existed and operated in the US oil according to Former Candidate Robert Junior Kennedy see Exhibit D.**

**The main issue here is as LTC Ed Green said in the meeting: America took too long to acknowledge these injuries and our service members languished without care of Havana Syndrome. This is no different and even worse for law-abiding citizens non-official governmental.**

**This letters and Exhibits are to inform all of you Elected Officials : We want you to investigate this Evil Technology. We want you all to TAKE ACTION requested in the May 8 meeting held by the Homeland Security see Exihibit M9**

**'TAKE ACTION -TAKE ACTION -TAKE ACTION**

**Give RETRIBUTION-RETRIBUTION- RETRIBUTION.**

**AS HHS SECRETARY ROBERT KENNEDY JUNIOR IS GETTING READY TO INVESTIGATE SUCH LONG OVERDUE ORGANIZED CRIMES, BE READY TO WORK ALONG WITH HIM.**

**---- INVESTIGATE THOSE COMPLAINTS from All VICTIMS OR SURVIVORS.**

**--- WHO ARE RESPONSIBE FOR THIS ORDER OF INFLICTING ANY CITIZEN AND GIVE ORDER TO INFLICT OUR L A CITIZENS?**

**-----PROSECUTE THOSE PERPETRATORS fully OF THE LAW-NO ONE IS ABOVE THE LAW.**

**– BAN SUCH TECHNOLOGY WEAPONS ON HUMANS NOW &4 THE FUTURE AS ASAP AS COLORADO LAW**

**---- WE NEED PULSE RADIO FREQUENCY LIBERATION-NEED A HAVANA ACT**

**----A TECHNOLOGY TO DETECT THOSE SILENT UNSEEN WEAPONS INCLUDING IN OUR SCHOOL &COLLEGES**

**------VICTIMS AS ORDINARY CITIZENS SHALL RECEIVE CONSISTENT HEAHTH CARE AND DAMAGES COMPENSATION AS PER HAVANA ACT OF 2021**

**----ALLOW AND PROTECT WISTLEBLOWERS FR RETALLIATION TO COME FORTH WITH TRUE FINDINGS.**

**Yes, we want to tell you all there are thousands ordinary citizens that have been attacked with Havana Syndrome including Dr Len Ber a medical Doctor whom was diagnosed by the same Medical Doctor who diagnosed the Diplomats- Dr Michael Hoffer**

**AS HONORABLE CORREA said during the hearing, what you heard during this meeting was very disturbing no doubt but it is the tip of the iceberg.**

**In addition to these Silent and Unseen DIRECTED ENERGY WEAPONS those SURVIVORS, OVERCOMERS have been dealing with organized crimes MULTI- PAID PERSON OR NEIGHBOOR HARASSMENT such as that retard on top of me and many in my block cross of the street, on my left, down the block, the day care &on. Those perpetrators do received GIFTS and /or unkind Gifts.**

**WE DEALT WITH HOME BREAK-INS, VICIOUS SLANDERING, COMMUNICATION INTEREFENCE & MONITORED, ACTIVITIES /SERVICES INTERFERENCE, SUCH AS HOSPITAL, WORK RELATED, BANKS, SCHOOL LOANS, FOOD POISONING, INTERNET & CAMERA MANIPULATION, STAGED ACCIDENT / OTHER EVEN MENTIONED FIRE just to mention a few. They are interfering with ALL YOUR/ MY LIFE &your activities as described Karen Melton Steward a retired National Security Agency Intelligence Analyst for 28 years see #Exhibit F.**

**NO CORRUPTION/ COVER UP WILL STOP UNLESS THERE IS INVESTIGATION.**

**As Mr. SWALWELL said he has met with some victims and their statement was your life has changed completely, it turns it upside down; yes, life is disoriented, so TRUE. Their account is they do not want this to happen to someone else. And that is exactly my AIM here I don't want this to continue, I don't want others to be subject to this evil satanic crime NOT even the Gangs in Haiti who destroyed a whole country and unlimited innocent lives, nor on those who been inflicted us on this soil. I will rather give them death penalty if guilty.**

**My life consists of preaching the Gospel, help the vulnerable, advocate on behalf of the voiceless and take care of my great family & help my community.**

**Congressman Golman said there was a Public Report from the Government reported these attacks from foreign malign actor as both witnesses replied it is unlikely unless it is happening abroad as Mr. Growzen said. I firmly believe the same thing it is happening on our soil. I believe that subcontractors, companies or organization, agencies, private and non-private are carrying these attacks COVERTLY on our land including Our Law enforcement.**

**Yes, too many of us on this soil have been afflicted and been subject of this Evil Cruelty on this land. I am a Pastor, an Educator, an Advocate, a Mom, a Former NYC Candidate, I am NOT a member of the United States Officials but I have been subject of these cruel attacks for the past ten years. I also know Michelle Blondmonvile and her mother an Elderly a peaceful wonderful law-abiding citizen woman is been afflicted almost every day. This breaks my heart.**

**I do know also about the Targeted Justice Org. that may have a registry of names of non-Governmental employees afflicted with Havana Syndrome.**

**Moreover, the reason that the Government does not released the TRUTH not because that they are classified documents Congressman Mr Goldman but there are those within the Government carrying such Evil cruelty. Many are involved such as government agencies, universities, government subcontractors and on the private sector as well, the utilities companies such as Con ED, The Internet Companies in my case Optimum, National Grid & on.**

**The Bible clearly said that the enemy is disguised; the enemy will NEVER appears as the enemy unless it got caught**

**We have a Mafia operating on this soil with multitude secret agents in every sector, every agency including all genders and ethnicities operating covertly destroying innocent Lives. They are coerced people to join their mafia club perhaps such people are afraid to decline for fear of their own lives. That is WHY we need to encourage whistleblowers to come forth and protect them against retaliation.TO STOP THEM & SAVE LIVES.**

**No one on the planet Earth will convince me otherwise, I have been going through this Evil ordeal for 14 years of my life. By God's grace, I am here to tell my story to save Lives and Rescue Lives to uproot Evil &his root in the name of Yeshua**

**This letter is to demand a CEASE and DESIST Immediately from all assault of microwave radiation, from any kind of remote or form of bio weapons or diabolical technology known as HAVANA SYNDROME against my body my life and to anyone else signed this letter.**

**We demand a cease of all assault of microwave radiation or any kind of remote technology harassment against my /our bodies from anyone in the three branches of the government or any private / non private agency or fusion center or NASA or any subcontractors, law enforcement agency ,utilities companies ,the Governor of NY if involves in such decision making to CEASE and DESIST IMMEDIATELY. I do not consent.**

**All exhibits A, B,C,D,M8,M9,E,F,G are a compilation of pictures, videos, picture of home breaking and information to support the statements on theses letter and to help the Elected Officials to locate the online information to save lives.**

**Thank You for your consideration**

**Email: adlkeb45@gmail.com / jesuschristheart@protonmail.com**

**Tel: 516 474 6119 / 3473127490 ( leave a message).**

**Pastor Adlerette Kebreau**

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 1684 & 450 Res. No. _____

☒ in favor ☐ in opposition

*Date:* 2/19/24

**(PLEASE PRINT)**

**Name:** Ivey Dyson

**Address:** _____

**I represent:** Brennan Center for Justice

**Address:** _____

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

*Date:* 2/19/25

**(PLEASE PRINT)**

**Name:** Colin Buckingham

**Address:** [redacted] Brooklyn NY 11226

**I represent:** _____

**Address:** _____

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. _____ Res. No. _____

☑ in favor ☐ in opposition

*Date:* _____

**(PLEASE PRINT)**

**Name:** Michele Bloodmorwille

**Address:** Queens NY

**I represent:** _____

**Address:** _____

*Please complete this card and return to the Sergeant-at-Arms*

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. ~~480~~ 480 Res. No. _____

~~☒~~ in favor ☐ in opposition

*Date:* 2/19/25

**(PLEASE PRINT)**

**Name:** Ivey Dyson

**Address:** ~~120 Broadway, Suite 750~~

**I represent:** ~~The Brennan Center for Justice~~

**Address:** _____

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

*Date:* 2/19/2025

**(PLEASE PRINT)**

**Name:** Pastor Adelette Kebreau

**Address:** Brooklyn NY

**I represent:** _____

**Address:** _____

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 480+168 Res. No. _____

☒ in favor ☐ in opposition

*Date:* _____

**(PLEASE PRINT)**

**Name:** David S. Scott

**Address:** 240 E 10th St, NY, NY

**I represent:** Surveillance Technology Oversight Project

**Address:** _____

*Please complete this card and return to the Sergeant-at-Arms*

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

*Date:* _____

**(PLEASE PRINT)**

**Name:** Jocelyn Strauber

**Address:** DOI Commissioner

**I represent:** 180 Maiden Lane

**Address:** _____

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. _____ Res. No. _____

☑ in favor ☐ in opposition

*Date:* _____

**(PLEASE PRINT)**

**Name:** Talia Kamran, ~~Brooklyn Defenders~~

**Address:** 177 Livingston St 7th Flr Bklyn 11201

**I represent:** Brooklyn Defender Svcs

**Address:** _____

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 165, 233, 480 Res. No. _____

☑ in favor ☐ in opposition

*Date:* _____

**(PLEASE PRINT)**

**Name:** Quincy Blair

**Address:** _____

**I represent:** Policing Project

**Address:** _____

*Please complete this card and return to the Sergeant-at-Arms*

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 0168-2024 Res. No. _____

☒ in favor ☐ in opposition

*Date:* 2.19.25

**(PLEASE PRINT)**

**Name:** Sergio De La Pava

**Address:** Legal Director

**I represent:** New York County Defender Services

**Address:** 100 William Street - 20th Floor

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. ~~168, 233, 480~~ Res. No. _____

☒ in favor ☐ in opposition

*Date:* 2/19/25

**(PLEASE PRINT)**

**Name:** Jerome Greco

**Address:** 49 Thomas Street, New York, NY 10013

**I represent:** The Legal Aid Society

**Address:** 49 Thomas Street, New York, NY 10013

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 480 168 233 Res. No. _____

☐ in favor ☐ in opposition

*Date:* 19 FEB 2025

**(PLEASE PRINT)**

**Name:** Cynthia Conti-Cook

**Address:** 121 6th Ave NY NY 10013

**I represent:** Surveillance Resistance Lab

**Address:** & Street Vendor Project

*Please complete this card and return to the Sergeant-at-Arms*

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 168, 233, 480 Res. No. _____

☐ in favor ☐ in opposition

*Date:* 02/19/2025

**(PLEASE PRINT)**

**Name:** Joshua Levin - Director Legislative

**Address:** affairs Unit

**I represent:** NYPD

**Address:** 1 Police Plaza

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 168, 233, 480 Res. No. _____

☐ in favor ☐ in opposition

*Date:* 2-19-2025

**(PLEASE PRINT)**

**Name:** Michael Gerber, Deputy Commissioner

**Address:** of Legal Matters

**I represent:** NYPD

**Address:** 1 Police Plaza

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 168, 233, 480 Res. No. _____

☐ in favor ☐ in opposition

*Date:* 2-19-2025

**(PLEASE PRINT)**

**Name:** Jason Savino - Commanding Officer of the

**Address:** Detective Bureau Specialty Enf. Div.

**I represent:** NYPD

**Address:** 1 Police Plaza

*Please complete this card and return to the Sergeant-at-Arms*

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. 233, 480 Res. No. _____

☐ in favor ☐ in opposition

*Date:* 2/19/25

**(PLEASE PRINT)**

**Name:** Commissioner Jocelyn Strauber

**Address:** [redacted] 180 Maiden Lane, NY 10038

**I represent:** DOI

**Address:** _____


# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*


I intend to appear and speak on Int. No. 168, 233, 476 Res. No. _____

☐ in favor ☐ in opposition

*Date:* 2-19-2025

**(PLEASE PRINT)**

**Name:** Captain Michael Eichner - Chief of Dept

**Address:** _____

**I represent:** NYPD

**Address:** 1 Police Plaza


# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*


I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

*Date:* _____

**(PLEASE PRINT)**

**Name:** ANDREW

**Address:** _____

**I represent:** SELF

**Address:** [redacted]

*Please complete this card and return to the Sergeant-at-Arms*

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

*Date:* 2/19/25

**(PLEASE PRINT)**

**Name:** Alex Stein

**Address:** [redacted]

**I represent:** Self

**Address:** Dallas TX 75209

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

*Date:* Feb 19, 2025

**(PLEASE PRINT)**

**Name:** Sharon Brown

**Address:** [redacted]

**I represent:** Rose of Sharon Enterprises

**Address:** 43 Madison Street 3F
Bklyn NY 11436

# THE COUNCIL
# THE CITY OF NEW YORK

*Appearance Card*

I intend to appear and speak on Int. No. _____ Res. No. _____

☑ in favor ☐ in opposition

*Date:* 2/19/25

**(PLEASE PRINT)**

**Name:** Christopher Leon Johnson

**Address:** [redacted]

**I represent:** Self

**Address:** _____

*Please complete this card and return to the Sergeant-at-Arms*