



Friday, December 15, 2023

**STATEMENT OF JEFFREY MADDREY
CHIEF OF DEPARTMENT
NEW YORK CITY POLICE DEPARTMENT**

**BEFORE THE NEW YORK CITY COUNCIL
COMMITTEES ON PUBLIC SAFETY AND TECHNOLOGY
COUNCIL CHAMBERS, CITY HALL
DECEMBER 15, 2023**

Good afternoon Chair Hanks, Chair Gutiérrez and Members of the Council. I am Jeffrey Maddrey, Chief of Department for the New York City Police Department (NYPD). I am joined by Deputy Commissioner for Legal Matters Michael Gerber and, on behalf of Police Commissioner Edward A. Caban, we appreciate the opportunity to speak with you today about the critical role that technology plays in keeping the city safe and the importance of transparency in the Department's use of technology.

From large-scale terrorist threats to every day street crime, technological advances play a pivotal role in solving and averting crime in New York City. NYPD technology supplements the best crime-fighting weapon we have at our disposal, the men and women of the NYPD who dedicate their lives to driving down crime and protecting the people of this City. The integration of technology into Department operations is not a matter of convenience; it is a necessity for the well-being of our communities and the officers who serve them. This has become more critical in recent years as we have seen a significant decline in staffing numbers. Technology provides a vital manpower multiplier and we must take steps to ensure our police are supported in the manner that is needed. Doing anything less would be irresponsible.

Take for example, our use of Unmanned Aerial Vehicles, or more commonly, drones. Before we had drones, we were forced to rely heavily on our helicopters for aviation support. Not only is deploying helicopters far costlier and more difficult to deploy than drones, but the severe noise from the helicopters disrupt the lives of every day New Yorkers. While there are times that helicopters are required, we can save significant resources and frustrations by using drones in certain situations, such as searching for missing persons, responding to hazardous conditions and crime scenes, assisting in crowd assessment at any number of large-scale events, such as New Year's Eve, J'ouvert and the West Indian Day parade, the Heritage of Pride parade and even monitoring for sharks at the city's beaches.

Here are some examples that perfectly illustrate how utilizing drones can be incredibly beneficial to the Department and to the community. The Electric Zoo Festival that took place in September was oversold by quite a bit and concerns arose over dangerous overcrowding. However, our officers on the ground, myself included, were not able to properly assess the crowd levels since they could only see the edge of the crowd. Our TARU personnel were able to deploy a drone over the crowd, and we were able to get a birds-eye view of what was really going on inside the gates. Rather than send in officers to disband the crowd and effectively shutting the festival down based on incomplete information, we were able to determine that, contrary to initial reports, there was ample space for all of the festivalgoers. Rather than taking drastic action, which may have risked

the safety of officers and attendees, our officers used the information gathered from the drone to direct the crowd in a safe manner. Having the ability to fly the drones allowed the festival to go on without having to send in additional officers and disrupting the event. Conversely, during the recent situation where a crowd lost control in Union Square, drones were vital in helping our people on the ground understand the nature and geography of the crowd. This time, we were able to properly deploy officers only to locations where they were needed to restore order. Additionally, we were able to utilize drones to track and ultimately apprehend individuals involved in an armed car-jacking. Drones were equally critical for on-the-ground commanding officers to understand the extent and nature of flooding during the storm a few months ago. It allowed the swift shutdown of flooded highways and the proper deployment of our resources. Drones have been used to assist our partners in the Parks Department to quickly identify whether or not a shark has been spotted, which when found, allows the Parks Department to keep people safe and when not found, allows New Yorkers to continue enjoying their day at the beach. Over Labor Day weekend, drones were deployed to provide assistance in the investigation of a shooting.

Additionally, StarChase has been used successfully to safely apprehend individuals accused of serious crimes. While still in the early phases of testing, it has led to 47 arrests of suspects fleeing police, allowing officers to safely follow and apprehend the individual. For instance, officers were investigating an armed robbery when the suspects fled. Utilizing StarChase, they were able to follow the vehicle at a safe distance while communicating with other officers. A separate team was able to find the vehicle, stop it and make two arrests. Without this technology, this could have resulted in the armed robbers escaping, allowing them to commit further crimes.

These are just two examples of the critical uses of technology which keep New Yorkers safe. I will now turn it over to Deputy Commissioner Gerber but I look forward to answering your questions.



Friday, December 15, 2023

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

**BEFORE THE NEW YORK CITY COUNCIL
COMMITTEES ON PUBLIC SAFETY AND TECHNOLOGY
COUNCIL CHAMBERS, CITY HALL
DECEMBER 15, 2023**

Good afternoon Chair Hanks, Chair Gutiérrez, and Members of the Council. My name is Michael Gerber, and I am the Deputy Commissioner of Legal Matters for the NYPD.

Since the POST Act was passed in 2020, the NYPD has worked to meet its obligations under the law. Within 180 days after the passage of the Act, the Department published 36 draft Impact and Use Policies, or IUPs, containing more than 300 pages of information regarding the Department's surveillance technologies. Following a comment period, the IUPs were finalized in April 2021. 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. The release of our IUPs, and subsequent amendments, have dramatically increased the Department's public disclosures regarding its surveillance technologies. The POST Act strikes a balance between a number of critical interests: transparency, public safety, innovation, and administrability. We disclose a wide range of information, without compromising our ability to solve crimes and keep people safe.

It has been suggested that we are grouping multiple surveillance technologies within a single IUP in a manner that undermines transparency. That is not the case. Within a given surveillance technology there will be different types of equipment and models, various forms in which the surveillance technology may be deployed, and a range of uses for that surveillance technology. We have not done a separate IUP and comment period for each type of hardware that deploys a given surveillance technology. Such an approach is not required by the POST Act. Having a separate IUP for each brand of camera that we use, or each variation on a given type of surveillance technology, would result in repetition and confusion. In fact, it would *decrease* transparency, as the nature of a particular surveillance technology used by the Department would be scattered across multiple IUPs. It would also be administratively unworkable. Itemizing surveillance technology used in covert operations would endanger public safety, provide a detailed road map to those who wish to do harm, and put our undercover officers at risk.

The POST Act accounts for all this. It makes clear that each surveillance technology must be covered within an IUP, but that enhancements to a surveillance technology, or the deployment of a surveillance technology for a new purpose or in a new manner, do *not* result in a new IUP and comment period. Rather, the Department is to write an addendum to a pre-existing IUP. I want to emphasize that in these circumstances, proceeding by addendum, rather than doing a new IUP, is not contrary to the POST Act. It is what the POST Act mandates, and it gives the Department

the flexibility to use preexisting surveillance technology in new ways while maintaining transparency with the public.

I would now like to take a moment to comment on the bills being heard today.

Intro. 1193 would require the Department to provide to DOI, upon request, a list of surveillance technologies, information on data access and retention policies, and quarterly updates on new and discontinued technologies. The Department takes DOI's oversight mission very seriously, and works with DOI to ensure that it can fulfill that mission. We are committed to continuing to do so. The Department looks forward to working with the Council to craft this legislation and to ensure that DOI has the information it needs to fulfill its audit function.

Intro. 1195 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 biannual audits 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 section of the patrol guide addressing facial recognition is posted on the Department's website, together with answers to frequently asked questions regarding our use of facial recognition. We have no issue with continuing to publicize this information, and we are open to providing more data regarding our use of this surveillance technology. We would, however, like to have a dialogue with the Council regarding the contours and scope of the audit. The bill as presently drafted requires granular detail regarding each itemized use of facial recognition technology that, at least at present, is administratively unfeasible and could interfere with our ability to use this important law enforcement tool. We believe that we can work with the Council to craft an audit that will further increase transparency without impeding critical law enforcement efforts.

Intro. 1207 would require 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 unsure what is intended by this language. Does this mean that every time the Department intends to purchase a different make or model of camera with even slightly altered functionality a new IUP would have to be issued? If we replace officers' smartphones, would a new IUP be required? Does this mean that the Department would be required to do an IUP for a new covert, undercover recording device? These are not rhetorical questions. The language of the bill, as presently drafted, is unclear. If the answer to these questions is yes, the bill would be extremely harmful to the functioning of the Department and could serve to compromise public safety. The Department opposes this legislation as drafted because it would upset the careful balance that lies at the heart of the POST Act.

We look forward to a continuing dialogue with the Council regarding the proposed bills and more generally regarding the POST Act. Thank you for the opportunity to testify on this matter, and we look forward to answering any questions you may have.



**NEW YORK CITY COUNCIL
JOINT HEARING BY THE COMMITTEE ON TECHNOLOGY AND
COMMITTEE ON PUBLIC SAFETY**

**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**

FRIDAY, DECEMBER 15, 2023

Good morning. My name is Jocelyn Strauber and I am the Commissioner of the Department of Investigation (“DOI”). Thank you, Chair Gutiérrez and members of the Committee on Technology, and Chair Hanks and members of the Committee on Public Safety, 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.

Today I will give you a summary of DOI’s findings from our first annual report pertaining to the POST Act, speak briefly about the focus of our second report which is currently in draft, and also share our view of the three proposed bills under consideration today with respect to the NYPD’s use of surveillance technology.

Before I begin, I want to recognize Inspector General (“IG”) Jeanene Barrett, who I appointed to the permanent position of Inspector General in August. Jeanene unfortunately could not be here today as planned, but I am very proud to be working with her. She has led the OIG-NYPD since January 2022 as the Acting Inspector General. She brings critical experience to this role in relevant areas including police oversight and accountability, community engagement, and supporting underserved communities.

November 2022 Report: An Assessment of NYPD’s Response to the POST Act

In November 2022, DOI issued its first report pursuant to the POST Act. The report was the result of an in-depth examination in which OIG-NYPD interviewed a range of individuals including NYPD officials, members of the advocacy community who called for the legislation that ultimately became the POST Act, and experts on various surveillance technologies. For this first report, the OIG-NYPD reviewed all published IUPs and performed a section-by-section assessment of one IUP, conducted an in-depth assessment of two selected surveillance technologies; and compared the POST Act to similar statutes in other jurisdictions to better understand other models for achieving transparency and public engagement in this area.

While the OIG-NYPD investigative team found that NYPD largely complied with the technical POST ACT requirements, it also found that the IUPs did not contain sufficient detail to allow for a full assessment of NYPD’s compliance with those IUPs, as the statute requires. OIG-NYPD concluded that improvements to the IUPs would enable more robust oversight, as well as more transparency with respect to the nature and use of these technologies. Specifically, the IUPs reviewed contained certain overly general language that failed to provide sufficiently specific information about the nature of the technologies, the retention period for data obtained via use of the technologies, and the entities with which the data can be shared. Per our assessment, the broad and non-specific language within the IUPs failed to provide clear direction to NYPD — and sufficiently concrete information to the public — in these and other areas.

Additionally, OIG-NYPD interprets the POST Act to require an IUP for each unique surveillance technology and disagrees with NYPD’s view that grouping is permitted as a general matter. While grouping may be appropriate for devices that use identical or very similar technologies, OIG-NYPD is concerned that grouping of related surveillance technologies into single IUPs is inconsistent with the spirit, if not the letter of the POST Act. Grouping may mask certain unique technological capabilities because they may not be publicly disclosed at all, as they will be deemed “covered” by an existing IUP. Furthermore, because there will be no new IUP applicable to those new technological capabilities, there will be no opportunity for public comment on those policies. It is also difficult for OIG-NYPD to meaningfully assess NYPD’s compliance with the IUP when the IUP applies to various technologies that could have different functions or capabilities.

Based on its review, OIG-NYPD issued 15 policy and procedure recommendations to NYPD in November of 2022. I want to be clear that many of these recommendations went beyond the requirements

that the POST Act imposes, and that we made these recommendations to enhance public transparency with respect to NYPD's use of surveillance technology. Equally important, the recommendations are intended to be sensitive to the need to protect confidential law enforcement information. For the most part, as the report made clear — with the exception of NYPD's practice with respect to grouping — we did not find that NYPD had violated the POST Act. The recommendations advised the NYPD to issue an IUP for each individual surveillance technology, to ensure that each IUP contains specific information such as the names of the entities with which the NYPD shares surveillance data as well as specific safeguards or restrictions on the use or dissemination of the surveillance data, and to describe the potential disparate impacts on protected groups of the use and deployment of the surveillance technology. OIG-NYPD also requested an itemized list of all surveillance technologies used by NYPD, in order to determine whether grouping of multiple devices or technologies under a single IUP was appropriate. NYPD previously rejected OIG-NYPD's recommendation to provide an itemized list of the surveillance technologies that it uses, and has since agreed to provide this itemized list. We look forward to receiving that list so that we can further consider the question whether any technologies currently grouped within a single IUP in fact require distinct IUPs.

The OIG-NYPD recommended that NYPD convene a working group that included NYPD personnel, relevant City Council members, and representatives from select advocacy groups who have expertise in surveillance technologies to make recommendations to NYPD on any necessary updates to existing IUPs, for example recommending updates to IUPs to reflect disparate impact of technologies. Other recommendations included strengthening internal tracking of each instance when NYPD provides an external agency with data collected via its surveillance technologies and other transparency measures.

With the exception of our recommendation that DOI receive an itemized list of technologies, NYPD has rejected all of our POST Act report recommendations.

DOI OIG-NYPD's Ongoing Role

DOI understands the relevant and important concerns about the use of surveillance technology in New York City and we are committed to providing oversight in this important area. I want to be clear that an annual comprehensive inquiry into the NYPD's compliance with each of its three dozen IUPs, for more than 80 surveillance technologies that it employs, is not a feasible undertaking for DOI. For that reason, both in last year's annual report and in the one we plan to issue in the first quarter of 2024, we are focused on particular surveillance technologies of public interest and concern, as well as broader issues with respect to the POST Act's requirements and NYPD's compliance more generally.

In our upcoming report we will discuss NYPD's compliance with the POST Act with respect to a group of technologies of particular public interest, including Digidog and the Autonomous Robot.

Proposed Legislation

DOI has reviewed Introductions 1193, 1195, and 1207, which are being considered at today's hearing, and is broadly supportive of the three bills as they generally track several of DOI's recommendations from the 2022 report. We look forward to working with the Council on these bills if they move forward to a vote.

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

Testimony by Comptroller Lander on NYPD's Implementation of the Public Oversight of Surveillance Technology (POST) ACT Before the New York City Council Committees on Public Safety and Technology

Thank you to Chair Gutierrez, Chair Hanks, and Members of the Committees on Technology and Public Safety for convening this important hearing on the New York City Police Department's (NYPD) implementation of the Public Oversight of Surveillance Technology (POST) Act and providing me the opportunity to testify.

As Chief Accountability Officer, the Comptroller's Office provides transparency and oversight of New York City agencies to promote integrity, strengthen trust, enable assessment, and identify opportunities to improve municipal operations to better serve New Yorkers. Technology offers powerful tools to increase government efficiency, but we must keep a close eye on the use of technologies that pose risks to democracy, privacy, and equity.

As a City Council member, I proudly co-sponsored and voted for the POST Act, with the goal to protect our civil rights and liberties through greater transparency of the NYPD's acquisition and deployment of new surveillance technology. I support the bills on today's calendar sponsored by Councilmembers Amanda Farias, Crystal Hudson, and Julie Won to ensure that the NYPD fulfills the spirit and letter of the POST Act.

The legislation being introduced today is responsive to the concerns raised by an investigation conducted by the Inspector General for the NYPD in their November 2022 report.

As the Inspector General's report noted, the NYPD has failed to publish the requisite Impact and Use Policies (IUP) for each surveillance technology used by the NYPD. Instead, the Department buried new surveillance technology under a single IUP that obfuscates what has been acquired and how it has been used. Furthermore, NYPD's practices do not allow for the POST Act's public notification process, which should enable 45 days for the public to submit comments on the NYPD's draft IUPs before finalization and deployment of new surveillance technology.

New Yorkers deserve more accountability as the Department continues to acquire and deploy surveillance technology in our communities. Intro 1207 tackles the way the Department has been drafting IUPs by clarifying that the NYPD is required to publish an IUP for each surveillance technology it uses, that the IUP identifies each external entity that receives data from said technology, that they report on safeguards to prevent dissemination of surveillance data, and that such IUPs adequately disclose assessment of potential disparate impacts on protected groups arising from the NYPD's use such technologies.

Together with Public Advocate Jumaane Williams, I sponsored the legislation that created the NYPD Inspector General's office in 2013 with the goal of empowering an independent oversight office to scrutinize NYPD policies and procedures, especially where civil rights and liberties are concerned. Intro 1193 by Council Member Farias and Intro 1207 by Council Member Won would enable the Office of the Inspector General for the NYPD (OIG-NYPD) to do that job by requiring the NYPD to provide the Department of Investigation (DOI) an itemized list of all surveillance technologies used by the Department, along with information on data access and retention policies for data collected by such technologies. Intro 1193 also requires the NYPD to provide DOI with quarterly updates on any newly acquired or discontinued technologies and updates to data access and retention policies.

These bills are vital to ensuring that the NYPD is implementing the POST Act as intended, bringing transparency to New Yorkers, and enabling oversight of surveillance technologies that carry with them risks to civil rights and liberties. With the rise of facial recognition technology in particular, which has repeatedly been shown to make disproportionate errors in identifying people of color, Intro 1193, sponsored by Council Member Hudson, would require the Department to publish a written policy establishing the procedures and regulations for the use of facial recognition technologies on its website and a biannual audit by the Department and a mandate to share its findings with DOI.

New Yorkers deserve to live in a safe and just city, and new technology of course has an important role to play in that work; however, law enforcement's increased use of surveillance technology tools without sufficient transparency and guardrails runs the risk of exacerbating inequity, violating privacy, and eroding the public's trust. We urge the Council to pass these bills to strengthen the POST Act and increase police accountability in New York City.

Thank you again for the opportunity to submit this testimony.



Legislative Affairs
125 Broad Street
New York, NY 10004
212-607-3300
www.nyclu.org

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

December 15, 2023

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”). 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 180,000 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.

Despite this clear, straightforward mandate, the NYPD – which was loudly on record in its opposition to the passage of the POST Act¹ – has remained stubbornly unwilling to comply. 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 policies themselves must also explicitly cover the “rules, processes, and guidelines ... regulating access to or use of such 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.

While we might expect that the NYPD to be reluctant to honestly account for the racially disparate impact of its surveillance practices, at minimum, the Department owes the public a

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 3 (2022), https://www.nyc.gov/assets/doi/reports/pdf/2022/20PostActRelease_Rpt_11032022.pdf [hereinafter OIG-NYPD REPORT].

⁴ *Id.* at 34.

⁵ See N.Y.C. Admin. Code § 14-188.

basic acknowledgement of the risks and an explanation of any efforts to mitigate those risks. Instead, the NYPD's policies 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, but 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 On 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.

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” land 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 demonstration of the NYPD's disregard for the transparency interests at the core of the POST Act, 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 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 OIG-NYPD noted, “the most logical reading of the POST Act's language is that it requires an IUP for each

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.

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 requested 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 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 Without City Council action to address these issues, the NYPD may seek to evade to any new notice and comment periods in the future, which is all the more troubling given this administration’s intense focus on expanding the NYPD’s technological capabilities.

OIG-NYPD’s 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 The NYPD rejected all but one recommendation – and even there, noted that that would merely “consider” a recommendation to issue a press release to announce the publication of, and comment periods related to, any future IUPs.¹⁴ Indeed, the NYPD has among the worst track records when it comes to city agencies accepting and implementing recommendations for Department of Investigation reports, with an analysis from *The City* finding that the NYPD has accepted only

⁸ 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 OIG-NYPD REPORT at 37.

¹⁴ CARRIE B. TALANSKY, NYPD RESPONSE TO AN ASSESSMENT OF NYPD’S RESPONSE TO THE POST ACT, NYPD (2022).

67% of recommendations since 2014 and outright failing to implement many recommendations that it purports to accept.¹⁵

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. Given the NYPD's failure to implement even that basic level of transparency, it is clear that further legislation is needed. The NYCLU supports Intros. 1207 and 1193, which would effectively codify many of the recommendations from OIG-NYPD's report.

Intro. 1207 would explicitly name the outside entities 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. 1193, 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 original intent of it – 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.

¹⁵ Reuven Blau & Suhail Bhat, *Department of Ignored: Agencies Refuse to Heed Hundreds of DOI Recommendations*, The City, Nov. 1, 2023, <https://www.thecity.nyc/2023/11/01/agencies-refuse-doi-recommendations/>.



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

Tel (718) 254-0700
Fax (718) 254-0897
info@bds.org

TESTIMONY OF

**Elizabeth Daniel Vasquez,
Director, Science and Surveillance Project**

BROOKLYN DEFENDER SERVICES

Presented before

The New York City Council Committees on Public Safety and Technology

Oversight Hearing on NYPD's Implementation of the POST Act

December 15, 2023

My name is Elizabeth Daniel Vasquez. I am the Director of the Science & Surveillance Project at Brooklyn Defender Services (BDS). BDS is a public defense office whose mission is to provide outstanding representation and advocacy free of cost to people facing loss of freedom, family separation and other serious legal harms by the government. I thank Chairs Hanks and Gutiérrez for inviting us to testify today about the NYPD's implementation of the Public Oversight of Surveillance Technology (POST) Act.

For over 25 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 22,000 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 NYPD's 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.

The City Council must not keep a firm oversight eye on NYPD’s surveillance programs.

The 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.² According to the NYPD, every other surveillance method can be deployed without any court approval or oversight.

Further, unlike other city agencies, the NYPD does not receive any significant public oversight through the contracting and procurement process. Despite the NYPD’s testimony to the contrary, the Department has fabricated for itself an agreed-upon workaround to the city’s fiscal oversight structure. Through the work of our colleagues at the Legal Aid Society, the public learned in 2021 that the NYPD was buying surveillance tools using city budget funds through a “Special Expenses Fund” that was exempted by internal agreements from oversight rules.³ This means that the public is unable to evaluate which companies and products NYPD has contracted with and for, the terms of that contracting (including data privacy provisions), and the amounts the NYPD has paid for

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 *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).

³ Sidney Fussell, *The NYPD had a secret fund for surveillance tools*, WIRED (Aug. 18, 2021), <https://www.wired.com/story/nypd-secret-fund-surveillance-tools/>.

these services per product or in the aggregate. The public has also been prevented from providing any input into these purchase decisions.

Further still, even if the City were to explicitly reject the PD's workaround and force transparency in contracting, PD is immune to the City's budget-related oversight as well. Over the past decades, significant surveillance tool purchases have been made through private donor funds funneled through the Police Foundation.⁴ While millions in city funds have been spent on these tools, additional undisclosed millions have flowed from unidentified donors to PD.

Rounding out this lack of external review and accountability, though the NYPD is technically subject to the watchdog oversight of the Office of Inspector General, this relationship has also been toothless in providing accountability. As discussed in more detail below, DOI's anemic approach to supervision is most on display in their failure to investigate NYPD's surveillance programming.

Finally, even simple statutory sunshine law provisions have failed when it comes to the NYPD. The NYPD fails to respond to freedom of information law requests, improperly invokes disclosure exceptions and exemptions when it does respond, and overall avoids transparency. As but one example, BDS' Science & Surveillance Project has at least two freedom of information law requests pending without response since 2019.

New York City has already invested more than \$1 billion in a twenty-year surveillance infrastructure building program.⁵ The city is blanketed in surveillance⁶ and no police department in the country has more military-grade surveillance resources than the NYPD. These tools—already heavily invested in and deployed—have done nothing to make New Yorkers safer or improve our city.⁷ All they have accomplished is to expand a burgeoning surveillance state, repeatedly infringing on New Yorkers' dignity, privacy, and First Amendment freedoms.⁸

⁴ Ali Winston & Darwin Bond Graham, *Private donors supply spy gear to cops*, ProPublica (Oct. 13, 2014) <https://www.propublica.org/article/private-donors-supply-spy-gear-to-cops>.

⁵ Ali Watkins, *How the N.Y.P.D. is using Post-9/11 Tools on Everyday New Yorkers*, NYTimes (Sept. 8, 2021) at <https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.htm>

⁶ See, e.g., Amnesty International, *Inside the NYPD's Surveillance Machine* at <https://banthescan.amnesty.org/decode/>.

⁷ Elizabeth Daniel Vasquez, *Opinion: Reining in the NYPD's Use of Surveillance Technologies*, City Limits (Feb. 22, 2022) at <https://citylimits.org/2022/02/22/opinion-reining-in-the-nypds-use-of-surveillance-technologies/>.

⁸ See, e.g., Elizabeth Daniel Vasquez, *Dismantle NYC's Mass Surveillance Project – Start with Jail Recordings*, Truthout.org (June 1, 2021) at <https://truthout.org/articles/dismantle-nycs-mass-surveillance-project-start-with-jail-recordings/>; James Vincent, *NYPD used facial recognition to track down Black Lives Matter activist*, TheVerge.com (Aug. 18, 2020) at <https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram>; Jan Ransom and Ashley Southall, *N.Y.P.D. Detectives Gave a Boy, 12, a Soda. He landed in a DNA Database*, NYTimes (Aug. 15, 2019) at <https://www.nytimes.com/2019/08/15/nyregion/nypd-dna-database.html>.

Take ShotSpotter as an example. In 2021, after an independent investigation conducted by journalists and academics, the Chicago Office of Inspector General’s Public Safety Section acted on the reported inquiry and data and conducted an investigation into the accuracy and deployment of the ShotSpotter system in the City of Chicago.⁹ The Chicago OIG concluded: “from its analysis that CPD responses to ShotSpotter alerts can seldom be shown to lead to investigatory stops which might have investigative value and rarely produce evidence of a gun-related crime. Additionally, OIG identified evidence that the introduction of ShotSpotter technology in Chicago has changed the way some CPD members perceive and interact with individuals present in areas where ShotSpotter alerts are frequent.”¹⁰

The technology deployed in New York City is identical to that deployed in Chicago. NYPD’s public statements regarding ShotSpotter’s deployment here—namely that deployment targets “high crime areas”—mimics precisely the Chicago Police Department’s statements about deployment. Despite our city’s investment in these listening systems, the data indicates that ShotSpotter is not resulting in a reduction in crime, but instead is contributing to over-policing in Black and brown neighborhoods.

Given this track record and the lack of data to support surveillance’s efficacy, this is not an area where NYPD should be written a blank accountability check. Instead, our city deserves *more* supervision, oversight, and regulation of this dangerous program.

The need for surveillance oversight has only become more urgent.

Twenty years after 9/11, a combination of security choices and technological advances (including increased processing speeds and decreased storage costs) have put our society on track to become a true surveillance state. Reliance on big data techniques is in vogue across all sectors. And since the late 1960s’ federal investment in the “professionalization” of policing elevated technology as the way forward in the criminal legal sector, law enforcement has wholeheartedly embraced surveillance technology as the future of policing.

Nowhere are these realities more true than in post-9/11 New York City.¹¹ We have outlined in prior testimony to the Public Safety Committee the breadth of technologies owned and deployed by the NYPD.¹² As a society, we are at an inflection point; data collection tools are now being met with amped up analysis tools turning eye-swimming piles of data into insights that can be readily processed and interpreted.

⁹ The City of Chicago’s Office of Inspector General, [The Chicago Police Department’s Use of Shotspotter Technology](#) (Aug. 2021).

¹⁰ *Id.*

¹¹ Ali Watkins, “[How the NYPD is Using Post-9/11 Tools on Everyday New Yorkers](#),” NYTimes (Sept. 8, 2021).

¹² See <https://bds.org/assets/files/City-Council-Mayors-Blueprint-Joint-Defender-Testimony-FINAL.pdf>

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.”¹³

City Council should not be persuaded by NYPD's distorted interpretation of the POST Act.

2023’s debut party for generative artificial intelligence only accelerates our societal chase. The Council should not be misled or confused by the NYPD’s attempts to manipulate linguistic squishiness to their advantage. In their testimony, the Department focused on the meaning of “surveillance technology” under the POST Act to argue that the intent of the statute was to require reporting around categories of surveillance.

The Act defined surveillance technology this way: “The term ‘surveillance technology’ means equipment, software, or systems capable of, or used or designed for, collecting, retaining, processing, or sharing audio, video, location, thermal, biometric, or similar information, that is operated by or at the direction of the department.” The Act then required Impact & Use Policies for “a surveillance technology” “at least 90 days prior to the use of any new surveillance technology.”

As technology advances, getting clarity on this language and its meaning will be critical to any notion of oversight. In its testimony, the NYPD focused on how onerous it would be to produce an Impact & Use Policy every time it purchased a new digital camera. But, by doing so, the NYPD obscured its failure to differentiate similar equipment, which may not require a new Impact & Use Policy, from analytics marketed under similar product categories, new collections of older tools, or genuinely different types of surveillance technologies contracted for, deployed by, or under development by the Department.

For example, despite this “grouping,” it is clear that the NYPD has failed to produce policies for all of its known surveillance technologies. We know of at least three critical surveillance technologies or tools that are entirely absent from the NYPD’s disclosures.

First, the NYPD has not submitted a proposed policy for its Rapid DNA Testing platform, despite telling the New York Commission on Forensic Science’s DNA Subcommittee more than four years

¹³ 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).

ago that the Department was developing and implementing such a platform.¹⁴[1] Relatedly, the New York City Council has held hearings on the operation of the NYPD's rogue local DNA database and its DNA collection policies. In partnership with the Office of Chief Medical Examiner, the NYPD acknowledged using the database as an investigative tool. The NYPD's POST Act impact and use policies make *no* mention of DNA: no mention of Rapid DNA testing, no mention of the database, no mention of NYPD's DNA collection practices including dragnet searches, and no mention of the NYPD's tracking within the Domain Awareness System of whether an individual is included in the DNA database or not.

Second, the Department has not submitted a policy for the Organized Crime Database that it told the City Council it used to track groups such as the Proud Boys, Ku Klux Klan, and Hells Angels.¹⁵ Expressly questioned about its gang database and its racialized definition of "gang," the NYPD asserted that it tracked groups like the mafia in an Organized Crime Database due to the groups' interstate ties. Leaving aside the NYPD's non sequitur about interstate operation, the failure to include the Organized Crime Database here raises larger concerns about the absence of tools the NYPD uses through or in conjunction with federal authorities amongst its disclosed technologies.

Third, the Department has not submitted a proposed policy for its access to Securus Technologies' Investigator Pro, THREADS, Guarded Exchange, or ICER. The City of New York's Department of Correction clearly has a contract with Securus for the provision of phone services on Rikers Island and in the other city jail facilities. Through that contract, the city purchased a voice biometric telephone system. It is also clear that the NYPD's "Fusion Team" has access to those Securus tools and technologies, and had a contract with Securus as of 2014. However, none of the Department's proposed policies discuss voice recognition, jail call monitoring, or any of Securus's other capabilities like location monitoring for external callers. Similarly, the Department does not mention other private corporate partners, like Vigilant Solutions, Palantir, Elucd, or Clearview AI, in their proposed policies.

Under the plain terms of the POST Act, the NYPD was required to submit surveillance policies for **all** of its surveillance technologies—even those used through or in conjunction with local or federal partners or private vendors.

The 36 policies issued by the NYPD are—at best—incomplete and misleading.

Of the surveillance policies that the NYPD has published, nearly every one is filled with copied-and-pasted, boilerplate stock language that fails to provide the City Council or the public with any

¹⁴ Kevin Deutsch, Exclusive: NYPD Plans to Use Controversial "Rapid DNA" Technology as Early as 2019, Bronx Justice News (Feb. 22, 2019), <https://bronxjusticenews.com/exclusive-nypd-plans-to-use-controversial-rapid-dna-technology-as-early-as-2019/>.

¹⁵ Nick Pinto, NYPD Added Nearly 2,500 New People to its Gang Database in the Last Year, The Intercept (June 28, 2019), <https://theintercept.com/2019/06/28/nypd-gang-database-additions/>.

meaningful information about the Department’s surveillance capabilities or activities. In fact, one could be forgiven for mistaking the NYPD’s 36 proposed policies for one policy that has been published 36 separate times. This form drafting process has multiple deleterious effects: first, it elides the substantial differences amongst technologies; second, it promotes sloppiness and allows for troubling errors; and third, it omits context and ignores connectedness to avoid dealing with the true threat of big data itself.

Across widely divergent surveillance technologies, the NYPD’s policies recycle the same copied-and-pasted language. Regardless of whether the policy is for a simple handheld tape recorder or a more sophisticated Stingray cell-site simulator, the “External Entities,” “Policies and procedures relating to public access or use of the data,” “Training,” and “Disparate impacts of the impact & use policy” sections *all consist of largely the same generalized language that fails to account for the technology being discussed.*

It defies common sense to think that the NYPD’s decision of whether to share an image taken from a CCTV camera should be guided by the same policy as its decision whether to share the far more invasive and personal information taken from a person’s cell phone, but that is exactly what the NYPD’s proposed policies suggest.

The NYPD’s decision to ignore significant differences in its surveillance technologies and the rules that should govern their use speaks to the Department’s deeply troubling failure to meaningfully engage with the POST Act.

Moreover, the NYPD’s policies contain a substantial amount of misleading or incomplete information. Perhaps most shockingly, the Facial Recognition, License Plate Reader, Domain Awareness System, and Social Network Analysis Tools policies each originally claimed not to “use artificial intelligence, machine learning, or any additional biometric measuring technologies.” These statements were either false or display a strange use of language, and the NYPD must have known it. When confronted with these falsehoods, the NYPD chose to merely delete mention of artificial intelligence and machine learning entirely.

However, the NYPD has become one of the leading proponents of these technologies precisely because of their artificial intelligence and machine learning capabilities.¹⁶ Facial recognition and license plate readers’ reliance on complex and often opaque algorithms have also led to numerous

¹⁶ See 2016 Edelman Finalist NYPD, YouTube (Feb. 1, 2017), <https://www.youtube.com/watch?v=dOwu4SMbVI4> (NYPD explaining at 1:30 how the Domain Awareness System uses artificial intelligence); Ryan Mac, Caroline Haskins, & Logan McDonald, Clearview’s Facial Recognition App Has Been Used by the Justice Department, ICE, Macy’s Walmart, and the NBA, BuzzFeed (Feb. 27, 2020), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement> (reporting that the NYPD “have run more than 11,000 searches, the most of any entity” despite having no policy to govern the use of the technology).

academic studies, complaints, and proposed legislation highlighting their racial bias.¹⁷ It is simply unbelievable that the NYPD does not understand how its own facial recognition software, license plate readers, social network analysis tools, and Domain Awareness System operate, particularly in light of the concerns and criticisms that have been raised in response to the Department's use of the technologies and the NYPD's own public claims.¹⁸

The NYPD chose to continue this misleading stance in its testimony to this Council by testifying again on Friday that they do not use artificial intelligence or machine learning.

Incredibly, the Facial Recognition policy contains an additional error that suggests the NYPD's proposed surveillance policies were written to check a box rather than guide and properly guide the Department's surveillance efforts. After making the dubious claim that facial recognition software does not use artificial intelligence or machine learning, the policy goes on to state that "when an investigator obtains an image depicting the face of an unidentified suspect, victim, or witness, and intends to identify the individual using facial recognition technology, the investigator must submit a request for facial recognition analysis." While this statement may reflect the NYPD's nominal policy, it does not reflect the Department's practice. As numerous media investigations and our own case experiences have demonstrated, there have been multiple instances in which NYPD officers have used backdoors to access facial recognition software without going through the process outlined in the policy.¹⁹ The policy does not address these incidents or explain how the Department will prevent similar incidents from happening in the future, and the NYPD's testimony on Friday further avoided reckoning with this reality. By failing to do so, the policy makes clear that it (and thus the other policies) does not reflect the realities of the NYPD's surveillance practices.

Other policies include false or misleading statements of another dimension. The proposed ShotSpotter policy, for example, claims that ShotSpotter "collects information on the *precise* time, location, and acoustic data of a potential gunfire incident." As reports have made clear and as NYPD's own internal documents indicate, however, the technology's accuracy is questionable as

¹⁷ See Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Oct. 18, 2016), <https://www.perpetuallineup.org/findings/racial-bias> ("The research that has been done [on facial recognition algorithms] ... suggests that these systems do, in fact, show signs of bias."); S. Bill S79 (Sen. Hoylman), available at: <https://www.nysenate.gov/legislation/bills/2021/S79>.

¹⁸ New York City Algorithms Management and Policy Officer, *Implementing Executive Order 50 (2019) Summary of Agency Compliance Reporting (CY 2020)*, <https://www.nyc.gov/assets/oti/downloads/pdf/reports/ampo-agency-compliance-cy-2020.pdf>.

¹⁹ See Ethan Geringer-Sameth, *The NYPD's Facial Recognition Policy Leaves A Lot of Leeway the Department Says It's Not Using*, *Gotham Gazette* (July 22, 2020), <https://www.gothamgazette.com/city/9608-nypd-facial-recognition-policy-leeway-department-not-using-black-lives-matter-protests>. See generally Clare Garvie, Georgetown Law Ctr. on Privacy & Technology, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (2019), <https://www.flawedfacedata.com/>.

to location, acoustic data, and even the identification of a gunshot.²⁰ Ignoring these caveats, the NYPD's policy suggests a level of precision and accuracy beyond ShotSpotter's current capabilities.

In addition to these easily disproven misstatements, the policies also omit critically important information that the City Council and the public need in order to evaluate other claims the NYPD makes throughout its policies. For example, nearly every policy claims that the NYPD does not share information collected through its surveillance tools with federal immigration enforcement, but none of the policies address what information the Department shares through its data-sharing agreements with the Department of Homeland Security's fusion centers.²¹ More broadly, the POST Act requires the NYPD to disclose who the Department shares its surveillance data with, but only three policies—the CCTV; Cell-site Simulators; and License Plate Reader policies—actually provide any meaningful information about the recipients of the NYPD's data, leaving the City Council and the public to guess who else has access to our location information, social media activity, and other highly personal information the NYPD routinely collects from all of us.

The issues outlined above are not an exhaustive list of the problems with the NYPD's surveillance policies, but rather illustrations of the Department's concerning and unacceptable rejection of the POST Act. At every turn, the NYPD made the conscious decision to disclose the least amount of information it believed it could provide without running afoul of the POST Act. In doing so, the NYPD has undermined the POST Act's purpose of informing the legislature and the public about the surveillance activities the Department is carrying out in our name, while also asserting that the courts have a nonexistent role in oversight as well. And even more troubling, the NYPD demonstrated its belief that the City Council's effort to bring transparency and democratic accountability to the Department's vast and troubling surveillance network is illegitimate and unworthy of a serious response.

The NYPD's refusal to engage with the true threat of technologically encoded racism is unacceptable.

As a public defense organization that has witnessed firsthand the devastating impacts of the New Jim Crow era's mass incarceration and the systemic racism of America's criminal legal system specifically on the communities we serve in Brooklyn, we are particularly troubled by the surveillance policies' complete failure to engage with the threat that the NYPD's surveillance technologies pose to Black and brown New Yorkers.

²⁰ See Matt Drange, "ShotSpotter Alerts Police To Lots Of Gunfire, But Produces Few Tangible Results," Forbes (Nov. 16, 2016), <https://www.forbes.com/sites/mattdrange/2016/11/17/shotspotteralerts-police-to-lots-of-gunfire-but-produces-few-tangible-results/#729e5b13229e>.

²¹ Department of Homeland Security, Fusion Center Locations and Contact Information, <https://www.dhs.gov/fusion-center-locations-and-contact-information>.

Every surveillance policy contains the same unpersuasive boilerplate claim that the policy will “mitigate the risk of impartial and biased law enforcement” and that “[t]he NYPD is committed to the impartial enforcement of the law and to the protection of constitutional rights.” The NYPD’s repetition of this claim does not make it true. Not only does the claim fail to meet the POST Act’s requirement that the NYPD address the racial inequities created by its surveillance technologies, but it also demonstrates the Department’s failure to think critically about how it will address, reduce, and eliminate the racism inherent in its current surveillance practices.

The NYPD’s professed commitment to so-called impartial law enforcement is insufficient under the POST Act because it fundamentally misunderstands the necessity of the anti-racist lens and the meaning of disparate impact.

The Department’s proposed policies ignore the different ways surveillance technologies are racially biased.²² For example, one form of racial bias associated with surveillance technologies occurs because the technology’s programming and development itself has rendered it inherently biased against Black and brown people. This bias can either emanate from the invisibility of Black and brown communities or the hyper-visibility of those same communities. A prime example of the invisibility effect has been facial recognition software. Study after study has demonstrated that the facial recognition systems used in the United States are least accurate when used on young Black women and most accurate when used on older white men.²³ The reason for this bias lies in the choices made in developing the facial recognition system itself: the data sets used to train the facial recognition algorithms fail to include a diversity of images resulting in algorithmic bias.

Another dimension of racial bias infecting surveillance technologies is the impact of data sets biased in the other direction: hyper-visibility. A prime example of this hyper-visibility effect has been predictive policing algorithms. Given the NYPD’s racist track record, such as its ongoing use of stop-and-frisk primarily against Black and Latine New Yorkers, the data sets used to train and develop any predictive policing system will inevitably reproduce racially biased outcomes.²⁴ The reason for this garbage-in-garbage-out bias lies in the choices made in developing the predictive policing system itself: the data sets used to train the predictive policing algorithms were collected in a biased manner to begin.

Beyond the development of surveillance technology, another common racial justice concern arises in the deployment of the technology post-development. Specifically, the threat presents itself that

²² For a more comprehensive discussion of the ways in which law enforcement surveillance technologies may replicate, mask, transfer, and exacerbate racial bias, see Laura M. Moy, *A Taxonomy of Police Technology’s Racial Inequity Problems*, 2021 U. Ill. L. Rev. 139, 154–75 (2021).

²³ Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Information Forensics and Security 1789, 1789 (2012); see also *Perpetual Line-Up*.

²⁴ See, e.g., Rashida Richardson, et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 192 (2019).

the racism present within police departments will lead officers to use surveillance technologies in racially biased ways. A police department may, for instance, choose to deploy license plate readers in predominantly Black and brown neighborhoods, leading it to gather huge amounts of information on some neighborhoods but not others. This form of bias helps explain the state of the NYPD’s “Gang Database,” which consists almost entirely of Black and Latine New Yorkers.²⁵

The NYPD’s surveillance policies deploy boilerplate language that glosses over these important distinctions amongst infection points for racial bias, making it impossible for the policies to actually address these persistent and obvious forms of racial bias.²⁶ At a moment of profound reckoning in America, these policies’ abject failure to engage with the racism inherent in police surveillance—and even the outright denial of its existence—unmasks the falsity of the NYPD’s professed “protect and serve” mission. And it demonstrates the NYPD’s dangerous refusal to engage with the racial equity concerns raised in academic literature and popular press and voiced at rallies across the country.

DOI’s Office of Inspector General for the NYPD is not presently an oversight solution capable of reckoning with the NYPD’s surveillance program.

Launched in 2014, the Office of Inspector General for the NYPD was tasked by the City Council with “the goal of enhancing the effectiveness of the department, increasing public safety, protecting civil liberties and civil rights, and increasing the public’s confidence in the police force, thus building stronger police-community relations.”²⁷

Since its inception, the OIG-NYPD has issued a total of 17 reports. Only two of those reports have addressed the impact of NYPD’s bloated surveillance apparatus on civil liberties and civil rights or the public’s confidence in the police force. This is a grave mistake.

As a civilian body vested with broad investigatory powers, it is the role of the OIG-NYPD to explore systemic issues within the NYPD that perpetuate biased policing, have a disproportionate impact on Black, brown, and low-income communities, and escape other structures of oversight and accountability. Despite this set of duties, the OIG-NYPD has presided over an era of expanded and expanding police technological armament without conducting any investigations into that growth.

The Public Oversight of Surveillance Technology (POST) Act of 2020 was passed by the City Council to increase transparency around the NYPD’s growing surveillance arsenal. The POST Act required the NYPD to publicly publish impact and use policies for each surveillance technology

²⁵ Nick Pinto, NYPD Added Nearly 2,500 New People to Its Gang Database in the Last Year, *The Intercept* (June 28, 2019), <https://theintercept.com/2019/06/28/nypd-gang-database-additions>.

²⁶ See Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (2019).

²⁷ Local Law No. 70 § 1.

the Department owned. Those policies were required to address not only capabilities and implementation, but also information about the disparate impact of the technologies' use.

In ostensible compliance with the POST Act, the first set of draft disclosures from the Department were published on January 11, 2021. Following a 45-day comment period, the Department then issued final disclosures on April 11, 2021. During the public comment period, multiple commenters and entities noted that the NYPD's disclosures were inaccurate, were essentially copy-and-paste jobs, and fundamentally failed to comply with the POST Act's requirements.²⁸ Many of these public comments were sent directly to the Department of Investigation, in addition to the NYPD.

Even without these public comments and filed grievances about the NYPD's failure to comply with the law, the POST Act itself requires the OIG-NYPD to prepare an annual audit of the NYPD's POST Act disclosures, assessing compliance, describing known or suspected violations, and publishing recommendations. It took more than a full calendar year from when the NYPD first issued their final disclosures for the OIG-NYPD to publish its legally required annual audit of the PD's disclosure. Prior to publication, the OIG-NYPD did not publicly reach out to commenters who raised concerns about the NYPD's POST Act compliance or conduct any external investigation.

Even without direct legislative direction to investigate the NYPD's use of science and surveillance technology, it is clear that the OIG-NYPD has and *should have* broader obligations of oversight and investigation in this space than the Office is currently acknowledging. The abysmal pace of the Office's investigations and the startling lack of creativity in identifying, opening, and pursuing investigations calls into question the effectiveness of the DOI's OIG-NYPD itself.

The NYPD's response to the final audit report's recommendations—rejecting all of them—made clear that OIG-NYPD POST Act oversight is currently toothless and in need of further legislative support. We support the Council's efforts to strengthen OIG-NYPD, as well as efforts to ensure its independence from the NYPD and other political influences.

We must move beyond technology-focused legislative philosophies to focus on the data.

The NYPD's insistence on grouping its surveillance technologies into 36 categories did have one positive impact: it highlighted our collective need to look not merely at individual technologies but instead to focus on the surveillance system as a whole.

²⁸ See, e.g., Public Comments submitted by Brooklyn Defender Services; [a Coalition of Advocates and Academics](#); [the New York Civil Liberties Union](#); [the Electronic Privacy Information Center](#); and [the Legal Aid Society](#).



When we view the entire network of surveillance—described by the NYPD as “incomparable to other law enforcement and public safety agencies”—we see a constellation not of tools, but of databases, which connectedly contain *billions* of data points.

To build an artificial intelligent (AI) system, the NYPD needs a large amount of data. Features of surveillance data—like locations, times, and descriptions—form the datasets needed to “teach” their AI tools. Without those datasets, tools like license plate readers, ShotSpotter, facial recognition, data analysis, social network analysis, digital forensic analysis, predictive policing, and other automated pattern recognition tools would be impossible.

This reality makes clear what has come into alarming focus for us: the biggest threat posed by surveillance in our city comes not from any single piece of technology, but instead from NYPD’s massive accumulation of data.

The NYPD’s web of interconnected systems together enables even more powerful forms of surveillance than each wields individually.

This is true because of artificial intelligence or AI. Put simply, the NYPD does not merely collect surveillance data to observe in the traditional sense. They also collect surveillance data to make predictions about New Yorkers, the future, and the past.

Because of the NYPD’s surveillance web, attacking just one piece of technology does very little. The only solution is to curtail NYPD’s data-collection capabilities and dismantle the surveillance infrastructure as a whole.

It is time for legislative solutions to focus on putting limits on the origination of records that include our personal data, the purposes for which that data may be used, and the length of time that data may remain in existence.

Conclusion

We thank the City Council for holding this important hearing today about the NYPD’s implementation of the Public Oversight of Surveillance Technology (POST) Act. If you have any questions, please feel free to reach out to contact me at evasquez@bds.org.

Testimony of the GANGS Coalition on NYPD Surveillance
NYC City Council hearing of the Committee on Public Safety and Committee on
Technology
12/15/2023

Good afternoon. We are The Grassroots Advocates for Neighborhood Groups and Solutions, known as the GANGS Coalition. We are a coalition of organizations and individuals that combats the over-policing and harassment of New Yorkers of color under the pretext of policing gangs and crews. Our Coalition includes young people, those who represent young people and who work with them through community-based organizations, and organizations striving to promote and protect their civil rights. We also conduct know-your-right sessions about surveillance. We are thus aware of the many ways that the NYPD collects information on our city's vulnerable youth and the impacts this has on their safety and well-being.

This policing, like the stop and frisk regime that it replaced, is racially discriminatory and weaponizes surveillance to stalk, track, and target young people of color and to collect information on these people in the Criminal Group Database (aka Gang Database) and other data repositories like the Domain Awareness System and Gun Recidivist Investigation Program (GRIP) list.

This surveillance is unconscionable for four reasons. First, the surveillance targets only Black and Latino New Yorkers who make up 99% of those in the Gang Database. Second, the surveillance is often achieved by the NYPD's use of fake social media profiles and phishing type scams to stalk young people and their friends. Third, while NYC is one of the safest cities in the world, and has historically low crime rates, gang surveillance and policing compromises public safety by increasing police interactions with young people, eroding the public's trust in law enforcement, and preventing already traumatized communities from building and strengthening social ties. And fourth, the surveillance fits squarely into a long and sordid history of race-based policing including Cointelpro, the harassment of the Black Panthers, post 9/11 surveillance of Muslim people in our schools, at their workplaces, and even in places of worship, and the NYPD's stop and frisk practices which peaked with over 685,000 stops in 2011. Will we ever learn from our history? Will we ever curtail the ability for the NYPD to surveil people without constraint or oversight?

First, if the NYPD's stop and frisk practices are racist—and they are, with about 90 % of those stopped being Black or Latino—the gang database is far worse. It is 99% Black and Latino. Although white supremacist groups represent the biggest threat to our democracy, they are not in the Criminal Group Database. No criminal activity or suspicion is required to be labeled a gang member. Allowing the police to simply collect information on anyone they like reinforces racial privilege. Most teens and adolescents hang out in groups, talk alike, dress alike, listen to the same music, and sometimes make errors in judgment that reflect their youth and immaturity. By labeling some youth as gang members and treating their conduct as a threat to society, we perpetuate racism and subject young people to unequal treatment based on race. The NYPD's Post Act Impact and Use Statement about the Gang Database utterly fails to address the issue

of racial bias in a database that is 99% Black and Latino New Yorkers, claiming in boilerplate language that "safeguard and audit protocols . . . mitigate the risk of impartial and biased law enforcement"^[1] despite the fact that there are no external safeguards or audits of the Criminal Group Database and internal protocols are not followed.^[2]

Second, the use of social media-based surveillance by the NYPD involves conduct that no parent would approve of. But the NYPD does not consult with parents, they do not consult with the City Council, nor do they provide notice to their targets. Instead, police gain access to private friend groups by creating fake profiles -- profiles of attractive young women, profiles using a friend's picture and name, or messages offering money if the recipient shares their CashApp information. Police gain access by demanding youth open their phones or share their passwords during street encounters, debriefs, and pretextual arrests for jay-walking and littering. Police will even pose as "Ops" posting messages to instigate conflicts and map groups. The online surveillance carries over into the streets. The young people that participate in our coalition and are represented by our groups do not feel safe anywhere, including public spaces in and around their homes and schools. They are stalked online. They are stalked outside: their buildings, courtyards, and recreational areas are deemed gang locations. This constant surveillance—and resulting frequent and escalated police encounters—results in feelings of isolation, instability, and fear of the police.

Third, as a matter of context, crime, violent crime, and youth crime in NYC are at historic lows.^[3] Crime was at historic lows in October 2012 when the NYPD first announced the launch of Operation Crew Cut, which doubled the number of officers assigned to track peer groups on social media.^[4] Neither crime in general, nor gang crime in particular, justifies the NYPD's investment in surveillance of youth of color, and in fact there were fewer gang motivated crimes each year in NYC than there were Gang Unit Officers assigned to Operation Crew Cut.^[5] Crime has continued at historic lows, with only an uptick during 2020 when schools and community centers were closed and summer youth employment suspended.

Why create, maintain and expand gang databases in a city with little violent crime and less gang crime? Operation Crew Cut was announced the month after the class action was certified in the stop and frisk case, *Floyd v. City of New York*. Rather than conduct surveillance by stopping Black and Latino men on the street in violation of the Fourth and Fourteenth Amendments, the NYPD expanded its investment in digital surveillance to collect information on people as young as 11 and 12.

While crime is at historic lows, investing in gang policing and prosecution actually creates public safety risks. Individuals who are labeled as gang members are more likely to go to jail and be exposed to violence and trauma and to be denied off-ramps like alternatives to incarceration or restorative justice. They are given long sentences. Jurisdictions that have invested in surveillance and gang policing, like LA and Chicago, have invested in intractable multi-generational gangs.^[6] NYPD's gang surveillance and suppression does not make this city safer. It almost certainly makes it less safe.

Finally, the NYPD's surveillance of young people of color by labeling them "threats" fits squarely into a long and sordid history of suspicionless police surveillance. That history includes the Cointelpro surveillance of Martin Luther King Jr, Malcolm X, Fred Hampton Sr, and the Black Panther Party among others. In New York City, we saw the surveillance of political activists that led to the *Handschu* Agreements, the post 9/11 surveillance of Muslim New Yorkers, and the resurgence of surveillance around the 2020 protests that saw the *Handschu* Agreement renewed. Indeed, NYPD documents indicate that officers are specifically monitoring "gang member" participation in protests and community events. We cannot allow the NYPD to engage in suspicionless and unsupervised surveillance of anyone, and most particularly vulnerable young people of color.

The GANGS Coalition asks the City Council to curtail the many unreliable and expensive surveillance technologies that the NYPD uses to profile vulnerable young people and instead invest in the arts, sports, after school and job programs, health services, violence interrupter sites, community gardens, affordable housing, and food assistance that reduce trauma and deprivation and truly safeguard our communities.

Most New Yorkers who are impacted by the NYPD's surveillance technology never even know that they are being monitored at all. These policing practices so often take place in the dark. Therefore, we support the transparency measures that the Council is considering today. However, we insist that transparency is not the ultimate goal, and we urge the Council to take further swift action to dismantle the oppressive surveillance technologies that ensnare entire Black and Brown communities, and our young people in particular.

[1] Criminal Group Database: Impact and Use Statement, p. 10 April 11, 2021. Available at. https://www.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/criminal-group-database-nypd-Impact-and-use-policy_4.9.21_final.pdf

[2] While not an "audit," the limited "investigation" by the OIG found that many entries in the gang database lacked sufficient documentation, that internal protocols were not consistently followed, sealed records were used in violation of the law, FOILS were routinely denied, among many other failures. An Investigation into NYPD's Criminal Group Database, April 2023. <https://www.nyc.gov/assets/doi/reports/pdf/2023/16CGDRpt.Release04.18.2023.pdf>

[3] At the time of this writing, murder is 80% lower than it was 30 years ago, and the seven major crimes tracked individually in weekly Compstat Reports are down over 70%. See NYPD Compstat Report Vol. 30 Number 22, covering the week ending 10/22/23. https://www.nyc.gov/assets/nypd/downloads/pdf/crime_statistics/cs-en-us-city.pdf

[4] For an analysis of crime and gang statistics when Operation Crew Cut was announced, see K Babe Howell, *Gang Policing: The Post Stop-and-Frisk Justification for Profile-Based Policing*, 5 U. DENV. CRIM. L. REV. 1 (2015). For specific numbers of "gang

[5] N.Y.C. Mayor's Management Report p. 4 (2013) available at https://www.nyc.gov/html/ops/downloads/pdf/mmr2013/2013_mmr.pdf

[6] Judith Greene & Kevin Pranis, *Gang Wars: The Failure of Enforcement Strategies and the Need for Effective Public Safety Strategies*, A JUSTICE POLICY INSTITUTE REPORT (July 2007), available at https://justicepolicy.org/wp-content/uploads/justicepolicy/documents/07-07_exs_gangwars_gc-ps-ac-jj.pdf

**NEW YORK CITY COUNCIL
COMMITTEE ON PUBLIC SAFETY
JOINTLY WITH THE COMMITTEE ON TECHNOLOGY**

HEARING:

Oversight – NYPD’s Implementation of the Public Oversight of Surveillance Technology (POST) Act

DATE:

October 11, 2023

TESTIMONY OF KATIE KINSEY
CHIEF OF STAFF, POLICING PROJECT AT NYU SCHOOL OF LAW

Honorable Members of the Committees on Public Safety and Technology of the New York City Council:

Thank you for calling this important public hearing to discuss the NYPD’s implementation of the Public Oversight of Surveillance Technology (POST) Act. In my testimony today, I want to make three points:

- First, I agree with the chorus of 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, I want to express support for the three amendments offered today that are designed to strengthen the Act’s disclosure requirements.
- Finally, I urge this body to pass an additional amendment that would do two things: (1) require City Council approval of NYPD’s Impact and Use Policies (IUPs); and (2) add enforcement mechanisms to ensure that the Act’s important transparency requirements have teeth.

But first, some brief background on our work. I’m an attorney at the Policing Project at New York University School of Law. Our organization’s mission is to “partner with communities and police to promote public safety through transparency, equity, and democratic engagement.”¹ Our work is focused on ensuring democratic accountability and public participation *on the front end*. By this we mean that the public has a voice in setting transparent, ethical, and effective policing

¹ *Our Mission*, Policing Project, <https://www.policingproject.org/our-mission>.

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 the sort of transparency that is essential to sound governance. In aiming to provide basic information to the public about the surveillance technologies that NYPD is deploying, and by requiring the NYPD to assess the impact of those technologies, this Act was intended to ensure an informed public debate about whether and how these powerful technologies should be used to keep New Yorkers safe. When a policing agency wants to use tools that are capable of identifying, tracking, and monitoring citizens' activities and whereabouts, the transparency envisioned by the POST Act should be the baseline. "Just trust us" is not a workable policy from an agency with a history of spying on ordinary people at mosques and using Stingrays to surveil protestors.²

We have no doubt that the POST Act's heart is in the right place, which is why we testified in favor of it at a hearing before this Committee in 2019. We likewise have no doubt that the NYPD broke this law's heart with its "general and generic" disclosure policy disclosures.³ The inadequacy of NYPD's Impact and Use Policy (IUP) disclosures is well-documented by reports from both the agency's own Inspector General's Office and the advocacy community alike.⁴

We will not re-tread that ground here, but we will note that the NYPD's flagrant disregard for this law's goals continues apace. Just this summer, the NYPD deployed an autonomous police robot with sophisticated surveillance capabilities in Times Square without first disclosing an IUP as required by this law.⁵ NYPD attempted to excuse this violation by claiming that these robots represented only an "enhancement[] to existing technologies" because it already uses stationary surveillance cameras.⁶ But as the NYPD well knows, there is no equivalence between a traditional stationary CCTV camera and a nearly 400-pound roving autonomous police robot. This robot is a new technology and as such it required a new IUP by law.

In its response to the OIG report detailing its inadequate disclosures, the NYPD protests that the report contains "no acknowledgment" that it has "exhibited a significant level of public

² Ed Pilkington, *NYPD settles lawsuit after illegally spying on Muslims*, THE GUARDIAN, (Apr. 5, 2018), <https://www.theguardian.com/world/2018/apr/05/nypd-muslim-surveillance-settlement>; Ali Winston, *Did the Police Spy on Black Lives Matter Protestors? The Answer May Come Out Soon*, N.Y. TIMES, (Jan. 14, 2019), <https://www.nytimes.com/2019/01/14/nyregion/nypd-black-lives-matter-surveillance.html>

³ See Jocelyn Strauber & Jeanene Barrett, *An Assessment of NYPD's Response to the POST Act*, OIG-NYPD (November 2022), https://www.nyc.gov/assets/doi/reports/pdf/2022/20PostActRelease_Rpt_11032022.pdf.

⁴ See generally *id.*; Eleni Manis & Albert Fox Cahn, *Above the Law? NYPD Violations of the Public Oversight of Surveillance Technology Act*, (Oct. 7, 2021), <https://www.stopspying.org/above-the-law>.

⁵ Ari Ephraim Feldman, *Critics call out NYPD surveillance robot over transparency concerns*, SPECTRUM NEWS NY1, (May 4, 2023), <https://ny1.com/nyc/all-boroughs/news/2023/05/03/critics-call-out-new-surveillance-robot-over-transparency-concerns>.

⁶ Chris Sommerfeldt, *NYPD robot Digidog reboot start of NYC tech push*, N.Y. DAILY NEWS (Apr. 12, 2023), <https://www.nydailynews.com/2023/04/12/mayor-adams-vows-nypd-robot-digidog-reboot-only-the-beginning-of-his-tech-push-amid-progressive-backlash>.

transparency surrounding its technologies prior to this law taking effect.”⁷ To support this claim, the NYPD cites some work we did with the agency in 2017 to help facilitate a public comment period around a new body-worn camera policy. Putting aside the fact that – against our recommendation – the NYPD did not follow public opinion on critical issues raised about that policy – soliciting public input one time, on one policy, for one technology, does not amount to a robust transparency practice around its technology use.

Although it is clear that NYPD has violated the spirit and intent of the POST Act, the agency has maintained repeatedly that its policy disclosures are “in compliance with the POST Act as written” and that OIG concluded as much.⁸ But even allowing for NYPD’s interpretation of the law’s IUP disclosure requirements, it is not the only requirement of the POST Act as written. The Act also empowers OIG with oversight responsibility to review NYPD’s actual use of surveillance technologies. Crucially, OIG also found that NYPD’s responses were “insufficient to enable OIG-NYPD to conduct full annual audits (as the Act also requires) and to achieve appropriate transparency with the public.”⁹

From OIG’s report, it is clear that the NYPD is not operating in good faith when it comes to its transparency responsibilities with the public. Fortunately for the citizens of New York, our democracy runs on laws not faith and this law can be amended to ensure robust transparency reporting is required. Members of this body already have taken steps to edit the law’s language to forestall any colorable argument from the NYPD that its barebones disclosures will be compliant moving forward. As such, we support the amendments proposed by Councilmembers Farías, Hudson, and Won and believe they will go a long way toward ending the NYPD’s brinkmanship.

Yet these amendments alone will not suffice to ensure New Yorkers receive the democratic accountability they deserve when it comes to their public safety. Meaningful democratic accountability requires this body to go one step further and amend the POST Act to include additional oversight and enforcement mechanisms.

Regarding oversight, the Council should amend the POST Act to require City Council approval of the NYPD’s IUPs. This way, the NYPD will not just get to set its own rules but rather will be accountable to democratically elected officials. In a recent survey of local surveillance ordinances like the POST Act, Berkeley Law found that only New York’s law lacked a requirement for elected-body approval of agencies’ surveillance policies and impact reports.¹⁰

⁷ Letter from Carrie B. Talansky, Acting Deputy Commission, Legal Matters, NYPD to Mayor Eric L. Adams et al., (Nov. 3, 2022), <https://www.nyc.gov/assets/nypd/downloads/pdf/oig-report-responses/nypd-response-2022-post-act.pdf>.

⁸ *Id.*

⁹ OIG-NYPD Report, *supra* note 3 at 4.

¹⁰ ARI CHIVUKULA & TYLER TAKEMOTO, LOCAL SURVEILLANCE OVERSIGHT ORDINANCES, SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC AT UC BERKELEY SCHOOL OF LAW 10 (2021), <https://www.law.berkeley.edu/wp-content/uploads/2021/02/Local-Surveillance-Ordinances-White-Paper.pdf>

Even a perfectly written statute will fail if it lacks effective enforcement mechanisms. Examples of enforcement mechanisms typically found in surveillance ordinances like the POST Act include a private right of action to sue the covered agency for violations; making it a misdemeanor for an official to intentionally violate the ordinance; including a suppression remedy to allow parties in lawsuits to exclude any evidence collected in violation of the ordinance; mandatory discipline for employees who violate the ordinance; and a termination or suspension of vendor contracts that violate the ordinance.¹¹ All of these enforcement mechanisms have merit. This body should amend the law to ensure at least one of these mechanisms is incorporated.

To be sure, there are technologies that play a valuable role in fostering public safety and the public actors entrusted with our safety should have access to them. Likewise, there certainly are some details about the police's use of certain surveillance technologies – for example, about tactical plans – that might not make sense to disclose publicly.

Neither of those truths, however, is inconsistent with the public's rights to information and accountability. Policing agencies should stop treating transparency and public safety as a zero-sum game. And legislative bodies like this one need to hold them to account.

¹¹ *Id.* at 13-16.



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

**STATEMENT OF
ALBERT FOX CAHN, EXECUTIVE DIRECTOR
AND NINA LOSHKAJIAN, STAFF ATTORNEY
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT (“S.T.O.P.”)**

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

**FOR AN OVERSIGHT HEARING ON NYPD’S IMPLEMENTATION OF THE
PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY (POST) ACT**

**PRESENTED
December 15th, 2023**

Good morning, Chair Gutiérrez, Chair Hanks, and members of the Committees on Technology and Public Safety. The Surveillance Technology Oversight Project (“S.T.O.P.”) is a New York-based civil rights and anti-surveillance group that advocates and litigates against discriminatory surveillance. Thank you for organizing this important hearing. We urge the Council to make NYPD surveillance reporting requirements enforceable and to ban police use of the most dangerous tools of police surveillance, including biased and ineffective facial recognition technology (FRT).

I. History of the POST Act and NYPD’s Noncompliance

The Public Oversight of Surveillance Technology (POST) Act, enacted in 2020, was the first New York City surveillance law since 9/11, and it required the NYPD to detail every technology it uses and how NYPD data is shared.¹ The law came in response to widespread outrage over the ineffectiveness, invasiveness, and cost of NYPD’s growing surveillance arsenal. Prior to the POST Act, the NYPD attempted to hide its use of invasive and creepy tools including StingRays, which mimic cellphone towers,² social media monitoring, Wi-Fi-based location tracking, the Domain Awareness System, and much more.³ Though the POST Act only required minimal transparency, that didn’t stop then-NYPD Deputy Commissioner from decrying the effort as “insane” and claiming the oversight law would become an “invaluable roadmap to criminals, terrorists, and others for how to harm the public.”⁴ Clearly, this has not been the reality, but the NYPD will continue to say that the sky is falling whenever it is held to even the lowest standard of accountability.

In reality, the importance of oversight of NYPD surveillance is indispensable given the Department’s sustained discrimination against BIPOC communities, Muslim New Yorkers, and LGBTQ+ New Yorkers. Surveillance technology amplifies historical policing biases, systematically surveilling low-income communities of color.⁵ Partnering with Amnesty International, we found: “the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras.”⁶

Thanks to the POST Act, billions of dollars in NYPD surveillance contracts previously hidden under the Special Expenses program were brought to light.⁷ The controversial secrecy agreement was terminated in 2020 in direct response to the POST Act’s passage. Working with the Legal Aid Society, we demanded the New York City Comptroller reveal records from the program and have exposed

¹ Public Oversight of Surveillance Technology (POST) Act, N.Y. CITY COUNCIL § 14-188 (N.Y. 2017), <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0>.

² *NYPD Has Used Stingrays More Than 1,000 Times Since 2008*, NYCLU, Feb. 11, 2016, <https://www.nyclu.org/en/pressreleases/nypd-has-used-stingrays-more-1000-times-2008>.

³ Ayyan Zubair, *Domain Awareness System*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, Sept. 26, 2019, <https://www.stopspying.org/latest-news/2019/9/26/domain-awareness-system>.

⁴ Nathan Tempy, *Top NYPD Official: Subjecting Our Surveillance Tools to Public Scrutiny Would Be ‘Insane’*, GOTHAMIST, June 14, 2017, <https://gothamist.com/news/top-nypd-official-subjecting-our-surveillance-tools-to-public-scrutiny-would-be-insane>.

⁵ Eleni Manis et al., *Scan City: A Decade of NYPD Facial Recognition Abuse*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, July 8, 2018, <https://www.stopspying.org/scan-city>.

⁶ *Inside the NYPD’s Surveillance Machine*, AMNESTY INTERNATIONAL, <https://banthescan.amnesty.org/decode>.

⁷ NYPD “Special Expenses” Contracts, Surveillance Technology Oversight Project, <https://www.stopspying.org/nypd-special-expenses>.

secret surveillance equipment that was hidden for more than a decade, including \$400 million on the Domain Awareness System.⁸

The POST Act was an essential first step in gaining greater transparency over the state of surveillance in New York City, but the NYPD has blatantly disregarded the requirements it imposes. The law does not set a high bar: NYPD is only required to disclose its surveillance tools and data sharing policies. Still, the NYPD has failed to clear even the low bar set by the POST Act. It failed to comply with the law’s reporting requirements with the draft “impact and use” policies published for public comment in January 2021, which consisted largely of boilerplate language not specific to each individual technology. NYPD then failed to respond to the public’s requests for more information when it published its revised policies in April 2021.

The impact and use policies required from the NYPD under the POST Act were meant to help the public and lawmakers gain crucial information on the Department’s surveillance practices. The consequences of NYPD’s spying are far-reaching, and therefore it is impossible to protect our communities without real insight. For example, because of NYPD’s secrecy, we don’t know what data ICE can access through fusion centers and other data sharing agreements, meaning we can’t ensure NYPD isn’t putting undocumented New Yorkers at risk of detention or deportation. We don’t know what private contractors get access to our info. And, terrifyingly, we don’t know how much bias the NYPD thinks is acceptable in its tools of mass surveillance, an incredibly disturbing state of affairs given the NYPD’s civil rights record.

Attached to this testimony as addendum A is a document containing S.T.O.P.’s organizational comments submitted to the NYPD in February 2021 in response to its initial publication of draft impact and use policies for public comment. These comments detail the lack of substance in the policies, including the lack of disclosure of vendors’ names, incomplete information on who can access the NYPD’s collected data, NYPD’s failure to meaningfully address whether tools had a disparate impact on protected groups, and missing definitions of artificial intelligence and machine learning, and more. S.T.O.P. also joined a coalition of concerned organizations who submitted a letter to the NYPD arguing that its draft policies demonstrated the department had failed to make a good-faith effort to comply with the POST Act.⁹ Unfortunately, when the NYPD published its revised policies in April 2021, they still fell short of the POST Act’s minimal requirements.¹⁰

II. NYPD Falls Short of the Standards Set by Other U.S. Police Agencies

The NYPD has shown the most egregious violations of the laxest law. NYPD’s failure to comply falls far short of the standards other U.S. police departments bound by similar measures have established. In our whitepaper titled “New CCOPS on the Beat: An Early Assessment of Community Control Over Police Surveillance Laws,” we performed a systematic review of all the Community Control of

⁸ *Id.*

⁹ *Coalition of Advocates and Academics Submit Joint Comments Documenting the NYPD’s Failure to Comply with the POST Act*, BRENNAN CENTER FOR JUSTICE, Feb. 24, 2021, <https://www.brennancenter.org/our-work/research-reports/coalition-advocates-and-academics-submit-joint-comments-documenting-nypds>.

¹⁰ Eleni Manis and Albert Fox Cahn, *Above The Law?: NYPD Violations of the Public Oversight of Surveillance Technology (POST) Act*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, Oct. 7, 2021, 6, https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/615df7245561b315e7289cee/1633548068620/2021.10.7_Above+the+Law_Research+Report.pdf.

Police Surveillance (CCOPS) laws in the country, and NYPD boasted the worst compliance record in the face of the weakest statute.¹¹ With New York City as a significant outlier, the report showed that many jurisdictions have—at least to some extent—seen increased transparency about and control over local law enforcement use of surveillance technology after passing a CCOPS ordinance. We followed up on this review with another whitepaper titled “Above The Law?: NYPD Violations of the POST Act” which further illustrated how NYPD has flouted its legal obligations.

Specifically, the Seattle Police Department provides names of specific vendors and models of technology. The NYPD only does so in two of its impact and use policies.¹² The Berkeley Police Department discloses each of the vendors with which it shares data and the City Manager of Cambridge, Massachusetts prepares an Annual Surveillance Report to the City of Cambridge that identifies the city’s surveillance technology vendors and the third-party entities with which it shares data collected by each technology.¹³ The NYPD, by contrast, only vaguely states that “[v]endors and contractors may have access” to surveillance technology “associated with software or data in performance of contractual duties to the NYPD.”¹⁴ The Berkeley Police Department provides concrete data retention periods in its policies,¹⁵ while the NYPD fails to provide specific timeframes in the majority of its policies.¹⁶ The bar for the NYPD is so low and they still trip over it.

¹¹ *New CCOPS on the Beat: An Early Assessment of Community Control Over Police Surveillance Laws*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT & HOGAN LOVELLS, LLP, Feb. 10, 2021, <https://www.stopspying.org/ccops>.

¹² *See, e.g.*, Seattle Police Department, Forward Looking Infrared Real-Time Video (FLIR) (KCSO Helicopters), Seattle Information Tech. (2020), <https://www.seattle.gov/Documents/Departments/Tech/Privacy/FLIR%20-%20KCSO%20Helicopters%20WG%20SIR.pdf> (listing the specific models and makes of its helicopters); Seattle Police Department, Automated License Plate Recognition (ALPR) (Patrol), Seattle Information Tech. (Jan. 31, 2019), [https://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20ALPR%20\(Patrol\)%20-%20Final%20SIR.pdf](https://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20ALPR%20(Patrol)%20-%20Final%20SIR.pdf) (identifying vendor of software); Seattle Police Department, CopLogic, Seattle Information Tech. (2019), <https://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20CopLogic%20Final%20SIR.pdf> (identifying specific software and vendor of surveillance technology).

¹³ Annual Surveillance Report, City Of Cambridge (Feb. 28, 2020), https://www.cambridgema.gov/-/media/Files/citymanagersoffice/surveillanceordinancedocuments/secondannualsurveillancereports_combined22820.pdf.

¹⁴ *See, e.g.*, Audio-Only Recording Devices, Covert: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/audio-only-recording-devices-covert-nypd--impact-and-use-policy_4.9.21_final.pdf.

¹⁵ *See, e.g.*, Berkeley Police Department, Surveillance Use Policy – Body Worn Cameras, City of Berkeley (Feb. 25, 2021), https://www.cityofberkeley.info/uploadedFiles/Police/Level_3_-_General/Surveillance_Use_Policy_-_Body_Worn_Cameras.pdf.

¹⁶ Closed circuit television systems, manned aircraft systems, and unmanned aircraft systems have a standard retention period of 30 days, subject to exception through the Retention and Disposition Schedule for New York Local Government Records. ClosedCircuit Television Systems: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/cctv-systems-nypd-Impact-and-usepolicy_4.9.21_final.pdf; Manned Aircraft Systems: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/manned-aircraft-systems-nypd-impact-and-usepolicy_4.9.21_final.pdf; Unmanned Aircraft Systems: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/unmanned-aircraft-systems-uas-nypd-impactand-use-policy_4.9.21_final.pdf. ShotSpotter has a retention period of 30 hours, subject through the Retention and Disposition Schedule for New York Local Government Records. ShotSpotter: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/shotspotter-nypd-impact-and-usepolicy_4.9.21_final.pdf. License plate readers have a standard retention rate of 5 years, subject to exception through the Retention and Disposition Schedule for New York Local Government Records. License Plate Readers: Impact and Use Policy, NYPD (Apr. 11, 2021),

III. OIG Report Proves NYPD’s Noncompliance

The POST Act requires the Office of the Inspector General (OIG) for the NYPD to annually audit NYPD compliance. In 2022, more than two years after the law was enacted, the OIG finally published its audit.¹⁷ The report detailed the NYPD’s many shortcomings and urged the NYPD to give both the OIG and the public greater information about how New Yorkers are surveilled. Stunningly, the OIG stated very clearly that it believed NYPD’s narrow interpretation of the POST Act undermines the law. Advocates and community members had been making this claim for years but, coming from another city agency, this was a landmark statement. Its other key findings were:

- NYPD used boilerplate language for its POST Act reports, hiding details of specific technologies;
- The NYPD largely failed to address the bias of its surveillance tools;
- The NYPD used blanket reports for multiple tools, once again detailed data for each technology; and
- NYPD failed to specify the specific safeguards / data sharing arrangements for each technology.¹⁸

In total, the OIG made fifteen specific and straightforward recommendations. The NYPD, however, only even considered implementing one—potentially issuing press releases when it publishes new impact and use policies—and rejected 93% of the advice in the OIG’s report outright, according to the OIG’s ninth Annual Report issued in March 2023.¹⁹ The NYPD’s blatant disregard for its obligations under the law makes it clear that the Council must take additional steps to rein in its abusive practices when it comes to surveillance technology.

IV. Need for Amendments and Bans on the Worst Police Surveillance

We urge the Council to listen to advocates and the OIG in taking urgent steps to ensure the NYPD follows the rule of law. Attached to this testimony as addendum B is a draft of legislation we support that would amend the POST Act to impose additional reporting and compliance requirements on the NYPD. This legislation can fix some of the loopholes the NYPD is currently exploiting, specifically by requiring a separate impact and use policy for each individual surveillance technology the department uses and the disclosure of which agencies have access to NYPD data. We also recommend the Council create a private right of action to make it clear that New Yorkers should have the right to sue the NYPD when they are violating the law.

This legislation would be crucial in creating some actual transparency and would also importantly alleviate the need for many ongoing lawsuits against the NYPD for its secrecy in using surveillance technology. Since the passage of the POST Act, we have filed nearly a dozen lawsuits stemming from

https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/license-plate-readerslpr-nypd-impact-and-use-policy_4.9.21_final.pdf.

¹⁷ *An Assessment of NYPD’s Response to the POST Act*, N.Y.C. DEP’T OF INVESTIGATION OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD, Nov. 2022,

https://www.nyc.gov/assets/doi/reports/pdf/2022/POSTActReport_Final_11032022.pdf.

¹⁸ *Id.*

¹⁹ *Ninth Annual Report*, N.Y.C. DEP’T OF INVESTIGATION OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD, March 2023, 5, <https://www.nyc.gov/assets/doi/reports/pdf/2023/13OIGNYDPRpt.Release.03.30.2023.pdf>

public records requests made to the NYPD. These lawsuits would not be necessary were the NYPD actually in compliance with the POST Act. For example, we represent Amnesty International USA (AI USA) in its lawsuit seeking NYPD records on its surveillance of historic Black Lives Matter protests in the summer of 2020, specifically records concerning the procurement, functionality, and general use of FRT, drones, gait recognition, cell-site simulators, and ambient sound recording devices. This litigation would not be necessary if the NYPD impact and use policies actually disclosed useful and detailed information.

Further, even if we are going to have the best transparency bill, it will not enough on its own to rein in the NYPD. Given NYPD’s obvious contempt for oversight in the three years since the POST Act’s passage, the Council must go further and ban police use of broken, biased surveillance technology like facial recognition, the so-called ‘gang database,’ and others. There are certain systems whose bias and ineffectiveness is already so well-documented that no additional information from the NYPD would justify their continued use. One such system is facial recognition.

We urge the Council to introduce a ban on government use of FRT, and to support Intros 1014 and 1024 banning use of FRT in places of public accommodation and residences. FRT is biased and error prone. Systems can be up to 99% accurate for middle-aged white men under ideal lighting in laboratory conditions but can be wrong more than 1 in 3 times for some women of color, even under similar conditions.²⁰ Numerous people, disproportionately Black, are wrongly arrested after being misidentified through facial recognition.²¹ Additionally, when facial recognition software can only recognize two genders, we leave transgender and non-binary individuals susceptible to misidentification and wrongful arrest.²²

Intro 1014 specifically prohibits any place or provider of public accommodation from using any biometric recognition technology to verify or identify a customer. It also prohibits businesses from barring entry to customers based on FRT and prevents companies from selling customers biometric data. This would be a crucial step towards protecting New Yorkers and preventing the types of abuses of the technology that we are seeing in places of public accommodation like Madison Square Garden, where owner James Dolan has vindictively used the incredible power of FRT to seek vengeance against his foes, blocking access to ticketholders who are affiliated with law firms involved in pending lawsuits against his company.

Use of FRT in residential settings opens tenants to harassment, discriminatory eviction, and compromises their privacy. New Yorkers do not want this invasive technology used in their homes, the most intimate of spaces.²³ Intro 1024 would prohibit any owner of a multiple dwelling from installing, activating, or using any biometric recognition technology that identifies tenants or the guest

²⁰ Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *Proceeds of Machine Learning Research*, vol 81, 1-15, 2018 p. 1.

²¹ Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES, Dec. 29, 2020, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

²² Rachel Mentz, *AI Software Defines People as Male or Female. That’s a Problem*, CNN BUSINESS, Nov. 21, 2019, <https://www.cnn.com/2019/11/21/tech/ai-gender-recognition-problem/index.html>.

²³ Yasmin Gagne, *How We Fought Our Landlord’s Secretive Plan for Facial Recognition—and Won*, Nov. 22, 2019, FAST COMPANY, <https://www.fastcompany.com/90431686/our-landlord-wants-to-install-facial-recognition-in-our-homes-but-were-fighting-back>.

of a tenant. The bill should be strengthened through amendments creating a strong private right of action applicable to all provisions, not just sale, with statutory damages and punitive damages, but its passage is critically important to make New Yorkers safer in their homes. Private FRT systems are just one 911 call away from being used by the NYPD, meaning these bills are also crucial to protect New Yorkers from false arrest and unwarranted police harassment.

A bill is urgently needed to ban police use of FRT as well. In this context, officers use pseudoscientific tactics that exacerbate the risk of error, such as running scans of celebrity lookalikes.²⁴ The Georgetown Law Center on Privacy and Technology documented the kinds of abuses that are “common practice” at NYPD.²⁵ One of the most egregious practices is that of routinely altering photos. The report revealed that NYPD edits of images “often go well beyond minor lighting adjustments and color correction,” and in many instances “amount to fabricating completely new identity points not present in the original photo.”²⁶ Police also abuse this tech to surveil protestors. There are reports that the NYPD used FRT to target Derrick Ingram for his leadership of a peaceful Black Lives Matter protest. Police later surrounded Derrick’s home with more than 50 officers as part of a retaliatory raid.²⁷

Because of its documented biases and its replication of historically flawed police practices, FRT should not be used by the NYPD or any other government agency. We call on the Council to introduce legislation banning all government use of FRT. In continuing to fail to act to ban the technology, New York falls further and further behind progressive cities from around the world.²⁸ Our coalition has been pushing these three FRT bills for over two years and it is long past time for the Council to protect New Yorkers by banning this dangerous technology.

The POST Act was a landmark bill because it reasserted the Council’s indispensable role in overseeing all NYPD operations, including its use of harmful surveillance technology like FRT. The Council must reassert its authority to ensure that the bill it fought so long to implement is not totally ignored.

²⁴ Khari Johnson, *NYPD Used Facial Recognition and Pics of Woody Harrelson to Arrest a Man*, VENTUREBEAT, May 16, 2019, <https://venturebeat.com/2019/05/16/nypd-used-facial-recognition-and-pics-of-woody-harrelson-to-arrest-a-man>.

²⁵ Clare Garvie, “Garbage In, Garbage Out: Face Recognition on Flawed Data,” Georgetown Law Center on Privacy and Technology, May 16, 2019, <https://www.flawedfacedata.com>.

²⁶ *Id.*

²⁷ George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology in Siege of Black Lives Matter Activist’s Apartment*, GOTHAMIST, Aug. 14, 2020, <https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment>.

²⁸ Shannon Flynn, *13 Cities Where Police Are Banned from Using Facial Recognition Tech*, INNOVATION & TECH TODAY, Nov. 18, 2020, <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech>; Kyle Wiggers, *AI Weekly: EU Facial Recognition Ban Highlights Need for U.S. Legislation*, VENTUREBEAT, Oct. 8, 2021, <https://venturebeat.com/2021/10/08/ai-weekly-eu-facial-recognition-ban-highlights-need-for-u-s-legislation>.



TESTIMONY

The Council of the City of New York
Committee on Public Safety & Committee on Technology

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

December 15, 2023

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

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

Diane Akerman
Digital Forensics Unit
Staff Attorney
(212) 298-5003
DAkerman@legal-aid.org

Contents

I. ORGANIZATIONAL INFORMATION	2
II. BACKGROUND ON THE POST ACT	2
III. THE NYPD SPECIAL EXPENSES (“SPEX”) BUDGET	3
A. The Original Memorandum of Understanding and Amendment	4
B. The POST Act Leads to the Dissolution of the Original Memorandum of Understanding and Amendment	5
C. A New Undisclosed Agreement	6
IV. ADDITIONAL POST ACT FAILURES	8
A. Unaddressed Issues with the Final NYPD Impact and Use Policies.....	8
B. The NYPD Office of the Inspector General First Annual Report.....	9
C. The NYPD Violated the POST Act in April and September 2023	15
1. <i>The NYPD Announces the Use of an Autonomous Security Robot, Digidog, and GPS Tracking Guns in April 2023</i>	16
2. <i>The NYPD Used Drones to Spy on Labor Day Celebrations</i>	18
D. The POST Act Does Not Prevent the NYPD from Purchasing or Using Invasive Surveillance Technology	20
1. <i>Facial Recognition Technology</i>	20
2. <i>Criminal Groups Database (aka Gang Database)</i>	23
3. <i>Social Media Monitoring</i>	24
V. THE BENEFITS OF THE POST ACT AND THE NEED FOR EXPANSION	25
A. Even Limited Transparency Has Helped Attorneys Properly Represent their Clients ..	26
B. If Followed Properly the POST Act Forces the NYPD to Engage with the Public about Its Surveillance Technology	27
VI. LEGISLATION TO FIX THE POST ACT	27
VII. CONCLUSION	32

Good morning. I am Jerome Greco, the Supervising Attorney for 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.

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, four staff attorneys, one paralegal, and one supervising attorney. 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.

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.” Int. 0487-2018 Summary.¹ 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.²

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.

III. THE NYPD SPECIAL EXPENSES (“SPEX”) BUDGET

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”)

¹ Summary of Int. 0487-2018, available at <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0> [last accessed Dec. 14, 2023].

² *Id.*

Budget. The SPEX Budget was used to secrete anything from mundane payments, like a \$3.88 check to a veterinarian for a shot for a police dog,³ to millions of dollars in surveillance equipment.⁴

A. The Original Memorandum of Understanding and Amendment

In 2007, the NYPD, the Law Department, the Mayor’s Office of Contract Services (MOCS), Department of Investigation (DOI), Office of Management and Budget (OMB), and the City Comptroller’s Office agreed to a “Protocol for Processing Special Expense Purchases for the NYPD.”⁵ This Memorandum of Understanding (MOU) set forth a process for how each of those city agencies would conduct their duties regarding SPEX budget purchases, but also avoid the legal requirements of public reporting at the same time. Some of the new policies included the DOI conducting Vendor Name Checks “off-line,” MOCS not filing VENDEX questionnaires in the public VENDEX database, and the Comptroller’s Office agreeing not to add SPEX procurements to the New York City Financial Management System (FMS). Additionally, the Comptroller’s Office was only permitted to retain a redacted version of the contract and other required documentation. Furthermore, the MOU allowed the NYPD to “set the target subcontracting percentage and participation goals at zero (0) percent” for the City’s Minority and Women-owned Business Enterprises (M/WBE) program. *Id.*

³ Graham Rayman & Rocco Parascandola, *EXCLUSIVE: NYPD vendors receiving nearly \$390M from budget shrouded in secret*, New York Daily News, Feb. 12, 2017, available at <https://www.nydailynews.com/2017/02/12/exclusive-nypd-vendors-receiving-nearly-390m-from-budget-shrouded-in-secret/> [last accessed Dec. 14, 2023].

⁴ Sidney Fussell, *The NYPD Had a Secret Fund for Surveillance Tools*, Wired, Aug. 10, 2021, available at <https://www.wired.com/story/nypd-secret-fund-surveillance-tools/> [last accessed Dec. 14, 2023].

⁵ *Protocol for Processing Special Expense Purchases for the NYPD*, Mar. 27, 2007, available at <https://archive.org/details/protocol-for-processing-special-expense-purchases-for-the-nypd-2007-03-27> [last accessed Dec. 14, 2023].

In 2010, the MOU was amended by an agreement between the NYPD, MOCS, and Comptroller's Office.⁶ The Amendment clarified which documents the Comptroller would be entitled to review, but did not change the restriction that the Comptroller's Office could only retain redacted copies. Also, the Amendment added an additional provision requiring the Comptroller to provide to the NYPD and MOCS, "a list of individuals who will be given authorization to review the NYPD confidential contracts, including name and title..."⁷

The original MOU and its amendment were obtained via a Freedom of Information Law request to the City Comptroller's Office by The Legal Aid Society in October 2020. As far as we are aware, they were not previously made public before our FOIL request.

B. The POST Act Leads to the Dissolution of the Original Memorandum of Understanding and Amendment

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.⁸ 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.⁹

The POST Act will help to bring some light to [NYPD surveillance] technologies, and in doing so it will also render moot a significant amount of the secrecy that the department has long insisted on bringing to the procurements it designates as classified, confidential special expenses. I recognize the need to take appropriate measures to protect the confidentiality of certain police

⁶ *Amendment to Special Expense Protocol*, June 18, 2010, available at <https://archive.org/details/amendment-to-special-expense-protocol-2010-06-18> [last accessed Dec. 14, 2023].

⁷ *Id.*

⁸ 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 Dec. 14, 2023].

⁹ *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 Dec. 14, 2023].

activities to ensure public safety as well as the safety of NYPD personnel. At the same time, I believe that it is time to terminate the MOU that has governed these purchases for more than a decade, and develop new processes that maximize transparency and accountability.¹⁰

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. While Comptroller Stringer's letter indicated that a new process or procedure would be developed in conjunction with the NYPD to replace the previous SPEX MOU and Amendment, no additional information was revealed publicly about any subsequent developments or agreements.

C. A New Undisclosed Agreement

Despite the enactment of the POST Act and the Comptroller's Office withdrawal from the SPEX MOU and Amendment, the NYPD has actively resisted providing copies of the contracts and related documents. Pursuant to separate FOIL requests filed by The Legal Aid Society and the Surveillance Technology Oversight Project (S.T.O.P.), thousands of pages of previously unreleased NYPD surveillance records were obtained from the City Comptroller's Office.¹¹ However, many of the pages were significantly redacted – some redacted to such an extreme that even the name of the company whom the NYPD contracted with was not revealed. Since the SPEX MOU and Amendment did not permit the Comptroller to retain unredacted copies of the SPEX related records, the Comptroller was unable to provide copies without redactions.

¹⁰ *Id.*

¹¹ Press Release, *S.T.O.P., Legal Aid Society Reveal Nearly \$3 Billion In Secret NYPD Surveillance Contracts*, Nov. 14, 2022, 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 Dec. 14, 2023].

The Legal Aid Society also sent a FOIL request to the NYPD for unredacted copies of the contracts and related records. The NYPD denied the request in full, which is unsurprising considering the NYPD's obvious disdain for FOIL and transparency, in general. 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.¹²

A hearing was held on the matter on July 10, 2023, in front of the Honorable Lyle E. Frank. Kevin Murtagh was the only witness to testify at the hearing. Murtagh is an Agency Attorney in the NYPD's Contract Administration Office. During his testimony, Murtagh revealed that there was a new agreement that replaced the prior dissolved SPEX budget MOU.

THE COURT: I have two questions. Just for clarification. So, like since 2020 what took its place? You have these contracts, all contracts are now confidential.

THE WITNESS: There was an agreement, Your Honor, where contracts were already in existence would continue to be treated confidentially. However, the issue is always the money and how we would track the money. So any new -- it took a long time to get there, but any new money, any new amendment or any new renewal would be done what we call the hybrid way. That it would not be put as part of the city record. We would not have hearings. It would be put in a FMS, which is Financial Management System, how money is tracked. That's the agreement we came to between us, MOCS and the Comptroller's office. In other words, it wasn't treated completely confidential any more, it was treated hybrid. Especially the money we tracked, that itself is put into the regular system tracking contract payments.

Transcript of Kevin Murtagh's testimony in the July 10, 2023 hearing, p. 51, lines 5 – 23.¹³

Murtagh revealed: (1) there is a new agreement between the NYPD, MOCS, and the Comptroller's Office to still deprive the public of oversight of the NYPD's spending on

¹² *The Legal Aid Society v. NYPD*, Index No. 156967/2021 (N.Y. Co. Sup. Ct.).

¹³ Upon request, The Legal Aid Society will provide a copy of the transcript.

surveillance technology; and (2) the new agreement still prevents any of the records previously covered under the dissolved older agreement to be released. It is disturbing that multiple city agencies continue to conspire to protect frivolous NYPD spending, and seek to weaken the already minimal requirements of the POST Act.

On October 27, 2023, the Court ruled in favor of The Legal Aid Society, requiring the NYPD to provide the requested records. However, the NYPD recently filed a notice of appeal, and the records subject to the trial Court's decision and order have not been turned over.

IV. ADDITIONAL POST ACT FAILURES

A. Unaddressed Issues with the Final NYPD Impact and Use Policies

On January 11, 2021, the NYPD published draft impact and use policies in alleged compliance with the POST Act. During the public comment period, numerous organizations and individuals submitted extensive comments about inadequacies of the policies, and their failure to fulfill the requirements of the POST Act. The Legal Aid Society alone submitted 47 pages of comments¹⁴ citing deficiencies in each of the policies – from issues as simple as failing to provide vendor information, to the more egregious failure to address the disparate impacts of the use of surveillance technology by the NYPD. Additionally, The Society submitted joint

¹⁴ The Legal Aid Society, *Comments on the NYPD Jan. 11, 2021 Draft Impact & Use Policies, pursuant to the Public Oversight of Surveillance Technology (POST) Act*, Feb. 25, 2021, available at <https://www.brennancenter.org/sites/default/files/2021-03/Legal%20Aid%20Society%20Comments%20on%20the%20Jan.%2011%2C%202021%20NYPD%20POST%20Act%20Draft%20Policies.pdf> [last accessed Dec. 14, 2023].

comments as part of the G.A.N.G.S coalition¹⁵ and with The Bronx Defenders, Center for Constitutional Rights, and the NAACP Legal Defense and Educational Fund, Inc.¹⁶

Despite the significant and robust commentary provided by organizational and community stakeholders, the NYPD finalized the draft policies without any substantial changes. In some cases, rather than addressing concerns from commentators, the NYPD simply removed any objectionable language.¹⁷ In drafting and finalizing the policies, the NYPD paid lip service to the letter and the spirit of the POST Act by using boilerplate language regardless of the technology at issue and their many well-documented flaws.

B. The NYPD Office of the Inspector General First Annual Report

The POST Act gives the Department of Investigation's Office of the Inspector General for the NYPD oversight responsibility and directs that the OIG-NYPD (1) assess whether the NYPD's use of surveillance technologies complies with published Impact & Use Policies (IUPs); (2) describe any known or reasonably suspected violations of the IUPs; and (3) publish recommendations, if any, relating to revisions of any IUPs. In November of 2022, the Office of

¹⁵ G.A.N.G.S Coalition, *Criminal Group (Gang) Database Impact & Use Policy*, Feb. 18, 2021, available at <https://twitter.com/GangScoalition/status/1362504164006367234> [last accessed Dec. 14, 2023].

¹⁶ The Bronx Defenders, et al., *Public Comment on the NYPD's Draft Impact & Use Policies for the Criminal Group Database and Social Network Analysis Tool*, Feb. 25, 2021, available at https://ccrjustice.org/sites/default/files/attach/2021/02/Written%20Comment%20on%20NYPD%27s%20Draft%20and%20Use%20Policies%20for%20the%20Gang%20Database%20and%20Social%20Network%20Analysis%20Tools_BXD_CCR_LAS_LDF.pdf [last accessed Dec. 14, 2023].

¹⁷ NYC Department of Investigation: Office of the Inspector General for the NYPD, *An Assessment of NYPD's Response to the POST Act* at 10, Nov. 2022, available at https://www.nyc.gov/assets/doi/reports/pdf/2022/20PostActRelease_Rpt_11032022.pdf [last accessed Dec. 14, 2023] (“the public comments highlighted that there is no industry-standard definition for ‘artificial intelligence’ and ‘machine learning’ (terms used in the draft IUPs)...In the final IUP, NYPD did not include a definition of these terms, but instead removed them entirely. While not in violation of the POST Act, this change heightened public suspicion that the Department’s IUPs were not transparent with respect to the surveillance technologies’ functionalities.”)

the Inspector General released their first annual report on the POST Act, “An Assessment of NYPD’s Response to the POST Act.”¹⁸

The OIG-NYPD noted broadly that the “the POST Act’s requirements establish the minimum with respect to disclosures” but “it does not prohibit the Department from providing additional information in the interests of transparency and good governance.”¹⁹ The OIG-NYPD’s assessment also found that the POST Act failed to meet community expectations or provide the robust protections of similar legislation in other jurisdictions. However, this failure is not solely the responsibility of the legislation, but rather, the NYPD’s opacity and deliberate misinterpretations of the requirements of the Post Act in order to undermine it. In particular, the report notes that “the vast majority of the IUPs produced by NYPD were general and generic in part...making it impracticable for OIG-NYPD to meaningfully assess the Department’s compliance with all the IUPs.”²⁰ The OIG-NYPD stated clearly that their position was that the “NYPD can and should provide additional information about these technologies, where doing so does not compromise the confidentiality of sensitive law enforcement disclosures” and included recommendations aimed at strengthening the law to meet its intended purpose.²¹

The OIG-NYPD made a number of findings – many of which reiterate the deficiencies outlined by organizations during the comment period.²² First, that though the NYPD “largely complied” with the POST Act’s requirements as to IUPs, simply meeting the requirements is insufficient to conduct full annual audits under the Act, or to achieve transparency with the

¹⁸ *Id.*

¹⁹ *Id.* at 15.

²⁰ *Id.* at 3.

²¹ *Id.* at 11.

²² *Id.* at 4 – 5.

public as to the use of the NYPD's surveillance technologies. Second, the IUPs included boilerplate language, and failed to provide sufficient specific detail. Third, the NYPD failed to address the potential disparate impacts of the use of most of the technologies under New York City Human Rights Law, addressing it in only 5 out of 26 of the IUPs. Fourth, the NYPD grouped technologies together, in spite of the POST Act's requirement to have an individual IUP for each technology. Finally, many of the ways the NYPD chose to interpret the requirements of the POST Act had the effect of allowing the NYPD to undermine portions of the law – both in letter and spirit. For example, claiming that similar technologies can be grouped together would allow the NYPD to effectively bypass the Act's public notification requirements prior to using a new technology. Presciently, the report uses the Digidog robot as an example of a technology that could potentially be deployed without any oversight based on the NYPD's reading of the law.

The report concluded by making fifteen recommendations intended to clarify and strengthen the POST Act, facilitate the OIG-NYPD's ability to conduct the required audits, and provide public transparency about the NYPD's use of surveillance technologies.²³ At the outset, the OIG-NYPD recommended that the NYPD convene a working group comprised of relevant City Council members, and representatives from advocacy and community groups with expertise in surveillance technology to make ongoing recommendations to the NYPD.²⁴ The OIG-NYPD then made specific recommendations intended to bring the NYPD into compliance with the POST Act, including issuing individual IUPs for each technology and ensuring that each IUP included or expanded on the following: identifying each external agency with whom the NYPD

²³ *Id.* at 6 – 7.

²⁴ *Id.* at 5.

shares surveillance data, the specific safeguards on the use or dissemination of surveillance data for each of those agencies, the potential disparate impacts on protected groups of the use and deployment of the technology itself, and identify safety hazards or lack thereof of each technology.²⁵

The OIG-NYPD also included a list of specific information the NYPD should provide to facilitate the completion of the required audit under the POST Act. First and foremost, the NYPD should provide the OIG-NYPD with an itemized list of all surveillance technologies employed and provide quarterly updates indicating which technologies have been newly acquired or discontinued.²⁶ Within 90 days, the NYPD should provide OIG-NYPD with information about the data collected by the various surveillance technologies, and within 180 days create an internal tracking system to record each instance where data is shared with an external agency.²⁷ The NYPD should provide information about which NYPD units maintain data collected by each technology, and the associated retention procedures.²⁸ More broadly, the NYPD should provide the OIG-NYPD with any and all data access and retention policies with the existing vendors who supply the surveillance technologies and provide information from new contracts quarterly.²⁹

The OIG-NYPD chose two of the most problematic surveillance technologies to illustrate the deficiencies of the IUPs and the NYPD's failure to comply with the POST Act – Facial

²⁵ *Id.* at 6 – 7.

²⁶ *Id.* at 7.

²⁷ *Id.* at 6.

²⁸ *Id.* at 6 – 7.

²⁹ *Id.* at 7.

Recognition Technology and Social Network Analysis Tools. The report compared the NYPD's use of FRT to best model practices for the use of FRT, particularly regarding modifications to probe photos, and found that "in contrast with the stringent model practices...NYPD did not report *any* guidelines to specify the types, orders, or numbers or modifications that could be conducted, and at what points in the alteration process searches should be run."¹⁵ The NYPD also uses Microsoft Paint and other unapproved programs that fail to track modification.³⁰ Even when using Adobe Photoshop, in accordance with model practices, the NYPD fails to utilize the Edit History Log, which would retain any changes to probe photos for review.³¹

In response to inquiries from the OIG-NYPD, the NYPD obfuscated and misrepresented findings and studies regarding the use of FRT. The FRT IUP acknowledges the existence of research about poor performance of the software in matching photographs from certain groups, but also notes that "an important federal government study on the subject" suggested that human review of FRT could alleviate those errors.³² The NYPD failed to cite the study in the IUP. When asked to provide the study to OIG-NYPD for the purposes of the report, the NYPD *misrepresented* the findings of a National Institute of Standards and Technology (NIST) study that had, in fact, explicitly stated that such a conclusion was "beyond the scope of the study."³³

NYPD's use of FRT also implicated a number of concerns about the NYPD's data and retention policies. The NYPD accesses the FRT program DataWorks Plus, through a portal provided by the United States Office of National Drug Control Policy ("ONDCP") New

³⁰ *Id.* at 26.

³¹ *Id.* at 26.

³² *Id.* at 27.

³³ *Id.* at 27 – 28.

York/New Jersey High Intensity Drug Trafficking Areas (“HIDTA”) program.³⁴ While the NYPD maintains certain records – records of a request made, the probe image, and the report from FIS – any other documentation of the use of FRT are controlled by HIDTA. This includes: the details of searches conducted, the likelihood that a probe image and possible match depict the same individual, and a log of modifications made to a probe image. All other information regarding the use of FRT is controlled by a third party. Even if the NYPD *had* a policy in place to conduct reviews of the use of FRT, it is essentially impossible for the NYPD or the OIG-NYPD to conduct any audit because all the necessary information lies in the hands of HIDTA and DataWorks Plus. More troubling, the NYPD’s agreement with DataWorks has absolutely no terms and conditions related to how data is retained, stored, and protected from disclosure, though such terms are not without precedent.³⁵ Again, the NYPD fails to even consider the privacy ramifications of surveillance technology and does not even bother to include standard, basic terms and conditions in contracts with outside vendors.

The OIG-NYPD also discussed social network analysis tools, noting at the outset that applicable IUP is misleading because the NYPD actually uses social *media* analysis technology.³⁶ Social network analysis refers to a limited tool, where social media analysis is a far more expansive technique that searches social media platforms using artificial intelligence. Numerous organizations have cited concerns with social media tracking as an invasion of privacy that also violates individual’s First Amendment right to free speech, and the freedom to

³⁴ *Id.* at 23.

³⁵ *Id.* at 28.

³⁶ *Id.* at 28.

assemble and protest.³⁷ Of concern is also the NYPD’s tactic of creating fake accounts using inappropriate lures to gain access to an individual’s posted information and social networks.³⁸

The IUP’s failures show exactly why the public is right to be concerned. First, in the IUP, the NYPD failed in any way to describe the specific social media analysis tool that is used – one that sweeps all major social media platforms for likely matches to an individual.³⁹ The IUP also stated that “information accessible to NYPD personnel using social network analysis technology is limited to publicly available information” which while *technically* true, fails to address the department’s regular practice of creating fake accounts to gain access to non-public information.⁴⁰ The NYPD has not promulgated guidelines on the appropriate use of these fake accounts, and does not create, maintain, or review any records regarding use of the tool.⁴¹ In fact, the NYPD does not *even know* whether the company that owns the program retains any records.⁴²

C. The NYPD Violated the POST Act in April and September 2023

The POST Act requires the NYPD to propose and publish an IUP on the department’s website “at least 90 days prior to the use of any new surveillance technology.”⁴³ The Public then shall have 45 days to submit comments on such policy to the NYPD Commissioner.⁴⁴ The OIG-

³⁷ *Id.* at 28.

³⁸ *Id.* at 28.

³⁹ *Id.* at 29.

⁴⁰ *Id.* at 29.

⁴¹ *Id.* at 29 – 30.

⁴² *Id.* at 30.

⁴³ NYC AC §14-188(b).

⁴⁴ *Id.* at (e).

NYPD’s report details the ways in which the NYPD creatively interprets the plain language of the POST Act to allow grouping technologies – rather than issuing individual IUPs for each technology – in an effort to avoid compliance and transparency. The report anticipated the ways that the NYPD could, and inevitably did, sidestep their requirements under the Act.

1. *The NYPD Announces the Use of an Autonomous Security Robot, Digidog, and GPS Tracking Guns in April 2023*⁴⁵

On April 11, 2023, the NYPD announced new surveillance technologies it would start using immediately. The NYPD neither drafted individual IUPs for each technology, nor provided for the mandatory 45 days for public comment. Instead, the NYPD quietly updated five of the thirty-six previously issued IUPs to reference the new tools. Just as the OIG-NYPD theorized, the NYPD’s “grouping approach” enabled the NYPD to “bypass the POST Act’s disclosure requirements for new technologies...and introduce new technologies under an existing group category...without the required public notification process – a critical aspect of the POST Act.”⁴⁶

In a press conference with Police Commissioner Keechant Sewell and Chief of Department Jeffrey Maddrey on April 11, 2023, New York City Mayor Eric Adams announced several new technologies that the NYPD acquired and intends to use going forward, either in pilot programs or permanently.⁴⁷ The Mayor discussed three new technologies:

⁴⁵ Legal Aid addressed the NYPD’s compliance failures in a letter to the OIG-NYPD in June of 2023. Press Release, Legal Aid Society, *LAS Demands Investigation Into NYPD Surveillance Technology Rollout*, June 14, 2023, available at <https://legalaidnyc.org/news/investigation-nypd-surveillance-technology-rollout/> [last accessed Dec. 14, 2023].

⁴⁶ *An Assessment of NYPD’s Response to the POST Act* at 36.

⁴⁷ Office of the Mayor, *Transcript: Mayor Adams Makes Public Safety Announcement With NYPD Commissioner Sewell*, The Official Website of the City of New York, Apr. 11, 2023, available at <https://www.nyc.gov/office-of-the-mayor/news/246-23/transcript-mayor-adams-makes-public-safety-announcementnypd-commissioner-sewell> [last accessed Dec. 14, 2023].

- A K5 autonomous security robot that is intended to patrol a “predetermined path” in areas such as subway stations.
- A return of Digidog, the dog-like remote-controlled robot that “will be able to enter, assess, assist the NYPD in tracking and investigating high risk hazardous situations and locations.”
- The StarChase GPS tracking guns. The NYPD is using two different versions of the StarChase GPS gun: a handheld device and a car-mounted device. Each launch a projectile with a live GPS tracker on it at a moving car. The GPS unit can then track the car, ostensibly in lieu of a police chase of the car.

These three technologies, plus two others that were not announced at this press conference, were incorporated into the NYPD’s existing technology IUPs on April 11, 2023. Five existing IUPs were updated, and no new IUPs were added for the new technology acquired by the NYPD. The two new technologies not announced at the Mayor’s press conference were:

- New digital fingerprint scanning technology that will allow officers to scan fingerprints straight from their cell phones.
- A new “augmented reality” technology available on some NYPD officers’ phones that will allow them to “better visualize that data [contained in the Domain Awareness System].”⁴⁸

Many of the new technologies unveiled in 2023 overlap IUP groups and have information in one IUP group that contradicts information in another, making clearer how necessary it is for the NYPD to release IUPs for each specific technology. The grouping allows technologies that

⁴⁸ Keechant Sewell, *2023 State of the NYPD*, YouTube, Jan. 25, 2023, available at <https://youtu.be/UyZjVz6w1n4?t=2049> [last accessed Dec. 14, 2023].

fall across IUP groups to be described minimally, and for the NYPD to withhold key information about the way these technologies work, the rules for deploying them, and the oversight of their use.

The NYPD's insistence on interpreting the POST Act to allow "grouping" of technologies is by itself an attempt to avoid transparency and oversight. But the interpretation has a more sinister effect – if a technology is not "new" it is then simply not subject to the 90-day waiting period, and 45-day comment period. It allows the NYPD to act without any public oversight when employing highly invasive technologies and to completely gut the legislative intent of the POST Act.

2. *The NYPD Used Drones to Spy on Labor Day Celebrations*

The inadequacies of the NYPD's policies for unmanned aircraft systems (more commonly known as drones) were again made apparent during this past Labor Day weekend. Before the holiday weekend, Assistant NYPD Commissioner Kaz Daughtry announced that the police would use drones in response to complaints about backyard parties: "If a caller states there's a large crowd, a large party in a backyard, we're going to be utilizing our assets to go up and go check on the party."⁴⁹ Essentially, the NYPD used drones to surveil Labor Day weekend barbeques occurring in the privacy of people's backyards in response to generic noise complaints.

⁴⁹ Jake Offenhartz, *New York police will use drones to monitor backyard parties this weekend, spurring privacy concerns*, Associated Press, Aug. 31, 2023, available at <https://apnews.com/article/drones-labor-day-eric-adams-nypd-jouvert-c2787e87bcad8fa87aa8d34b454ee6cf> [last accessed Dec. 14, 2023].

The NYPD Patrol Guide states that drones can only be used in “limited circumstances.”⁵⁰ Those limited circumstances are: (1) search and rescue operations; (2) documentation of collisions and crime scenes; (3) evidence searches at large or inaccessible scenes; (4) hazardous material incidents; (5) monitoring vehicular traffic and pedestrian congestion at large scale events; (6) visual assistance at hostage/barricaded suspect situations; (7) rooftop security observation at shootings or large scale events at the direction of the Incident Commander; (8) public safety, emergency, or other situation with the approval of the Chief of Department; and (9) pre-warrant execution safety survey and during execution of a search warrant, as appropriate.⁵¹ The NYPD’s Unmanned Aircraft Systems: Impact & Use Policy⁵² repeats these same limited circumstances as constraints on the NYPD’s drone capabilities.

Monitoring backyard parties and barbeques during a holiday weekend, which traditionally is celebrated by holding and attending such events, based solely on an unverified neighbor’s complaint about the size of the party or the noise generated from it does not fit within any of the listed “limited circumstances” that allegedly justify the use of a drone. A noise complaint is not even considered low priority and directed to 311, rather than 911. Even the incredibly broad discretion given to the Chief of Department (“public safety, emergency, or other situation with the approval of the Chief of Department”) could not justify a blanket policy change to spy on New Yorkers celebrating in their privacy of their backyards or the backyards of

⁵⁰ NYPD Patrol Guide Procedure No. 212-124, *Use of Department Unmanned Aircraft System (UAS)*. This Patrol Guide section was updated on September 22, 2023, after Labor Day weekend. Here, we are referring to the January 6, 2022 version because that was the version in place during the relevant time period. Moreover, the updated version does not resolve the issues discussed.

⁵¹ *Id.*

⁵² The Unmanned Aircraft Systems: Impact and Use Policy was updated on September 22, 2023, after Labor Day weekend. Here, we are referring to the April 11, 2021 IUP because that was the Policy in place during the relevant time period. Moreover, the updated Policy does not resolve the issues discussed.

their families and friends, otherwise there would be no limitations on when the NYPD could fly drones.

Furthermore, people have a reasonable expectation of privacy in their backyards and the areas behind their homes. Deploying a drone to spy upon people in these areas without a warrant is a violation of the U.S. Const., Amend. IV and the N.Y. Const., Art. I, §12. Even the Patrol Guide and the IUP acknowledge a warrant is required to use a drone to surveil areas where there is a reasonable expectation of privacy: “[a]bsent exigent circumstances, a UAS will **NOT** be deployed in areas where there is a reasonable expectation of privacy (e.g., to look inside of residences), without first obtaining a search warrant,”⁵³ and “[a]bsent exigent circumstances, a UAS will not be used in areas where there is a reasonable expectation of privacy without NYPD personnel first obtaining a search warrant that explicitly authorizes the use of a UAS.”⁵⁴

D. The POST Act Does Not Prevent the NYPD from Purchasing or Using Invasive Surveillance Technology

1. *Facial Recognition Technology*

The time has long since passed for legislators to ban the use of harmful facial recognition technology. There is simply no way to mitigate the biases and unreliability of this technology. The NYPD has also proven they cannot be trusted to utilize this technology in a way that mitigates harm – they continue to obfuscate their use of the software and refuse to implement any best practices. The NYPD have gone so far as to make repeated misrepresentations in their own IUP and upon direct questioning from the OIG-NYPD.

⁵³ NYPD Patrol Guide Procedure No. 212-124, *Use of Department Unmanned Aircraft System (UAS)* (emphasis in the original).

⁵⁴ NYPD Unmanned Aircraft Systems: Impact & Use Policy.

Facial Recognition Technology has now been responsible for numerous cases of false arrests and imprisonment as a result of false positives.⁵⁵ New York already lags behind other jurisdictions that have banned the use of FRT by both private entities and law enforcement.⁵⁶ Most recently, the New York State Education Department Commissioner banned the practice in schools after finding that “there were serious concerns regarding the use of FRT in schools, including...the higher rate of false positives for people of color, nonbinary and transgender people, women, the elderly and children” that were not “outweighed by the claimed benefits.”⁵⁷ The report by the commissioner also concluded that there is “little information is available about real life situations where such technology detected and helped prevent violent incidents.”⁵⁸

The NYPD not only insists on continued use of the technology but are willing to go to great lengths to hide its use and lie about its accuracy and reliability. The NYPD’s use of facial recognition technology, in particular the problematic software Clearview AI, was hidden from the public and uncovered from leaks to the media and in response to a FOIL request from The Legal Aid Society, and after numerous attempts to avoid disclosing the information.⁵⁹ Prior to

⁵⁵ Thanawala Sudhin, *Facial Recognition Technology Jailed A Man For Days. His Lawsuit Joins Others From Black Plaintiffs*, Associated Press, Sep. 25, 2023, available at <https://apnews.com/article/mistaken-arrests-facial-recognition-technology-lawsuits-b613161c56472459df683f54320d08a7> [last accessed Dec. 14, 2023].

⁵⁶ Fight for the Future, *Ban Facial Recognition Map*, available at <https://www.banfacialrecognition.com/map/> [last accessed Dec. 14, 2023].

⁵⁷ New York State Education Department Commissioner Determination on Biometric Identifying Technology in Schools, Sept. 27, 2023 available at <https://www.nysed.gov/sites/default/files/programs/data-privacy-security/biometric-determination-9-27-23.pdf> [last accessed Dec. 14, 2023].

⁵⁸ *Id.*

⁵⁹ The Legal Aid Society, *NYPD is Using Controversial Facial Recognition Software*, Apr. 8, 2021, available at <https://legalaidnyc.org/news/nypd-using-controversial-facial-recognition-software/> [last accessed Dec. 14, 2023].

these disclosures, the NYPD repeatedly and publicly denied use of the software.⁶⁰ The NYPD also often constructed alternate theories to mask the use of the technology and avoid revealing its use or any relevant discovery to defense attorneys. Despite the NYPD’s own protocols stating that facial recognition does not establish probable cause to make an arrest,⁶¹ arrests are often made based on scant evidence simply because of a facial recognition match. Though the discovery reforms of 2020 now mandate disclosure of documents relating to the use of FRT, and the NYPD Patrol Guide references the existence of “Case Notes” a Facial Investigation Section Officer must take, in practice these notes rarely if ever, exist. Even in the rare circumstance where notes are kept and provided, they in no way model the best practices outlined by the OIG-NYPD.

The NYPD’s dedication to the use of this faulty technology is so extreme, that they are willing to provide false information to the OIG-NYPD and the public.

In the FRT IUP, the Department acknowledged research highlighting poor performance by some algorithms in matching photographs of individuals from certain racial and/or ethnic groups, if the algorithms were not trained with respect to those groups. The IUP also noted “an important federal government study on the subject” that suggested that human review of FRT matches could alleviate such errors. This study, however, is not cited in the IUP. When asked for the study in connection with the preparation of this Report, NYPD claimed that a National Institute of Standards and Technology study presents evidence that “erroneous software matches can be swiftly corrected by human observers.” OIG-NYPD reviewed that study and concluded that it does not support NYPD’s claim that human observation can remedy erroneous software matches. *In fact, to the contrary, the study does not address human observation except to state that “the*

⁶⁰ Craig McCarthy, *Rogue NYPD Cops Are Using Facial Recognition App Clearview*, Jan. 23, 2020, available at <https://nypost.com/2020/01/23/rogue-nypd-cops-are-using-sketchy-facial-recognition-app-clearview/> [last accessed Dec. 14, 2023].

⁶¹ NYPD Patrol Guide Procedure No. 212-129, *Facial Recognition Technology*.

interaction of machine and human is beyond the scope of this [study], as is human efficacy.”⁶²

The OIG-NYPD released their report on the NYPD’s compliance with the POST Act in June of this year. Last month, the NYPD updated their FRT IUP, repeating its reliance on a NIST report, but still refusing to provide a cite to it or any study reaching a similar conclusion, and still failing to address the OIG-NYPD’s vastly different interpretation of the report. The NYPD simply continues to restate this erroneous assertion, even including it in a public NYPD webpage titled “NYPD Questions and Answers: Facial Recognition.”⁶³ They have proven that they are willing to find every loophole, commit the most extreme of linguistic gymnastics, to avoid compliance with any attempt to regulate their use of the technology. It is precisely this kind of behavior by the NYPD that necessitated the passage of the POST Act, and exactly the behavior that proves the NYPD cannot be trusted with this harmful technology.

2. Criminal Groups Database (aka Gang Database)

The NYPD’s use and reliance on the Criminal Group Database (“Gang Database”) is another area that clearly shows their failure to assess the disparate impact on protected classes of its surveillance technologies, as required by the POST Act. The recent report of the OIG-NYPD found that 99% of people in the database are Black and Latinx, and that a person can be placed in

⁶² *An Assessment of NYPD’s Response to the POST Act* at 27 – 28.

⁶³ NYPD, *NYPD Questions and Answers: Facial Recognition*, The Official Website of the City of New York, available at <https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page> [last accessed Dec. 14, 2023] (“Some studies have found variations in accuracy for some software products. **The most important federal government study on the subject**, however, noted that in ‘hybrid machine/human systems,’ where the software findings are routinely reviewed by human investigators, erroneous software matches can be swiftly corrected by human observers. The safeguards built into the NYPD’s protocols for managing facial recognition, which provide an immediate human review of the software findings, prevent misidentification.”) (emphasis added).

the database based on a single social media post.⁶⁴ The NYPD's IUP of the Gang Database was not only generic, but it also completely ignored the racially discriminatory criteria and arbitrary discretion that targets people of color to label them as gang members.

The OIG-NYPD report confirmed that the methods and practices for inclusion into the gang database were substantially flawed. These flaws highlight the discrimination that the database sanctions, a heightened surveillance of Black and brown communities based on association, appearance, and neighborhood. The report confirmed that people's residence in public housing served as a basis for inclusion.⁶⁵ It revealed that the database targets children as young as 11, based on non-criminal association and expression.⁶⁶ There was a lack of documentation for significant numbers of database entries according to OIG-NYPD's review of 500+ records. The database also uses sealed arrest records.⁶⁷ Together, these are systemic compliance failures under the POST Act because none of these methods were ever revealed in the NYPD's Gang Database IUP.

3. *Social Media Monitoring*

The NYPD's social media surveillance tools facilitate the criminalization of people by funneling their activity to label them as gang or crew members. The OIG-NYPD report also confirmed that the criteria for social media inclusion was vague and that the IUP "does not clarify the amount and nature of the evidence required to conclude that an individual satisfies the

⁶⁴ NYC Department of Investigation: Office of the Inspector General for the NYPD, An Investigation into NYPD's Criminal Group Database, Apr. 2023, available at <https://www.nyc.gov/assets/doi/reports/pdf/2023/16CGDRpt.Release04.18.2023.pdf> [last accessed Dec. 14, 2023].

⁶⁵ *Id.* at 46 – 47.

⁶⁶ *Id.* at 35.

⁶⁷ *Id.* at 41.

criteria for entry into the CGD.” For example, something as innocuous as wishing someone “Happy Birthday” on a monitored social media page could be used to classify them in the gang database.⁶⁸

These surveillance technologies permit the NYPD to constantly monitor the lives of Black and Latinx youth, through actual and digital “stop and frisk,” and in ways that subject these youth to racially discriminatory policing practices and inclusion into their gang database. Once your information is in the database, it is never removed. And if you are in the “active” portion of the database, any officer who looks up your name will be notified that you are member of a criminal gang. As the OIG-NYPD notes, if an officer stops a person for any reason, that officer can be notified through the Domain Awareness System (DAS) that the person is alleged to be a member of a criminal gang, increasing the likelihood of an extended search or detention.

The NYPD’s Gang Database IUP omitted the extent of its social media surveillance by not explaining the evidence used to enter people into the database, what other law enforcement agencies the NYPD shares the information with, and what guidance officers use to review the entries they make. The secretive practices of the Criminal Groups Database allow the NYPD to violate due process protections and engage in mass-criminalization of Black and Latinx people. The NYPD must eliminate its Gang Database, end its policies and practices that rely on the Gang Database or underlying criteria, and end digital surveillance policies and practices that disproportionately impact youth of color.

V. THE BENEFITS OF THE POST ACT AND THE NEED FOR EXPANSION

Although the POST Act has fallen short, both in its own limitations (e.g., not banning certain surveillance technologies) and in the NYPD’s malicious “compliance,” it still has

⁶⁸ *Id.* at 48.

provided valuable information. It can also be improved by expanding its provisions and by closing any perceived loopholes the NYPD has used to attempt to justify its lack of compliance.

A. Even Limited Transparency Has Helped Attorneys Properly Represent their Clients

Even with the NYPD's attempts to subvert the intent of the POST Act, their limited disclosures have been helpful to defense attorneys representing indigent people in criminal cases. Public defenders are always struggling to get more information about the investigations and evidence in their clients' cases, even after the recent reforms to the discovery law. This is further complicated by the NYPD's efforts to hide or obscure their use of surveillance. Sometimes, even prosecutors are unaware that a surveillance tool was used in a case because the NYPD failed to document it or failed to provide the district attorney's office with the required paperwork.

Though the NYPD's Impact & Use Policies are significantly flawed, the tiny bit of transparency they provide is used by attorneys to investigate their cases, litigate over missing discovery, and demand hearings to challenge surveillance methods and results. It is incredibly difficult to successfully argue about a technology you did not even know existed or for which there is so little information about how it functions that you do not know its purpose. Furthermore, it allows attorneys to educate the courts. For example, in *People v. Gutierrez*,⁶⁹ the Court relied upon the ShotSpotter: Impact & Use Policy, among other records, to decide that discoverable materials existed related to the ShotSpotter system and that they were in the custody and control of the prosecution:

While it is true that ShotSpotter is an independent entity, as the People assert, the policy statement makes it abundantly clear that the NYPD has access to a substantial amount of data, if not all of the data, generated and maintained by the company. In fact, the policy statement provides, "If ShotSpotter data is relevant to a

⁶⁹ 78 Misc. 3d 411 (Bronx Co. Sup. Ct. 2023).

criminal case, the *NYPD* will turn the data over to the prosecutor with jurisdiction over the matter,” not the company's discovery compliance unit (*id.* at 7 [emphasis added]). Thus, for all intents and purposes, most, if not all, of the ShotSpotter data may be deemed to be in possession of the police department.⁷⁰

It is important to note that the ShotSpotter policy is one of the few Impact & Use Policies that includes the name of the manufacturer and model of the surveillance tool. Without that information, the defense would be required to prove who produces the technology to show what records it generates, or we would be unable to specify what discovery may be available.

B. If Followed Properly the POST Act Forces the NYPD to Engage with the Public about Its Surveillance Technology

If the NYPD followed the POST Act requirements as written and as intended, it would force them to meaningfully engage with the communities that are most likely to be targets of these surveillance tools. Despite the POST Act's shortcomings, the information the NYPD is required to release could be used to help educate the public about how their taxes are being spent, how their privacy may be invaded, and their rights when such tools are used against them. Furthermore, this could generate discussion among community members about what they feel are appropriate practices to address issues that affect their community. However, the NYPD's clear disdain for the transparency coupled with the fact that they ignored many, if not most, of the criticisms of the draft Impact & Use Policies in the finalized versions, leads the public to believe that there is no value in engagement or pushing back – a goal the NYPD appears to seek.

VI. LEGISLATION TO FIX THE POST ACT

There are three bills that have been introduced to fix some of the flaws in the POST Act that this testimony discussed. Council Member Amada Farías has sponsored Int. 1193-2023:

This legislation would add new provisions to the law which would require that the NYPD, upon request, provide the Department of

⁷⁰ *Id.* at 423.

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.⁷¹

Council Member Crystal Hudson has sponsored Int. 1195-2023:

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 with the Department of Investigation, and post such findings on the Department's website.⁷²

Council Members Julie Won and Christopher Marte have sponsored Int. 1207-2023:

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.⁷³

⁷¹ Summary of Int. 1193-2023, available at <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6356879&GUID=4BA09060-C709-4E18-AA5F-60467D60CB40> [last accessed Dec. 14, 2023].

⁷² Summary of Int. 1195-2023, available at <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6356886&GUID=D0F0D52B-02D1-4248-8B8C-51421EB4B3B5> [last accessed Dec. 14, 2023].

⁷³ Summary of Int. 1207-2023, available at <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=6356887&GUID=C2CA4D2F-B2A0-4761-A151-9A10B9511D50> [last accessed Dec. 14, 2023].

All three bills are admirable in their attempts to prevent the NYPD from continuing their abuse of surveillance technology and hiding behind perceived loopholes in the original version of the POST Act. However, they are still missing some key requirements, without which the NYPD will succeed in continuing to thwart the goals the POST Act was intended to achieve.

We encourage the Council Members to adopt the following provisions in their bills to achieve the actual transparency and oversight the POST Act was meant to require. Some of the suggestions below are covered by one or more of the three bills introduced, but we have included all the provisions we urge to be passed for the convenience of both the Council and the public.

Section 1. Section 14-188 is amended to add a new subdivision g to read as follows:

g. Additional Reporting and Compliance Requirements:

1. The department shall issue a separate impact and use policy for each individual surveillance technology, particularly describing all information required under this subsection. Each piece of applicable equipment, software, and system shall constitute a separate, individual technology unless it is identical to another technology in every aspect of how it collects, stores, analyzes, and/or disseminates information
2. The department shall identify in each impact and use policy each external agency, by name, with which the department can share surveillance data and the extent of such data sharing, including, but not limited to, the method by which said agency accesses information collected, stored, analyzed, and/or disseminated by said technology, if such an agency can copy or retain information from said technology, and all entities with whom an external agency is known to share such information.
3. The department shall include in each impact and use policy the specific safeguards/restrictions on use or dissemination of the surveillance data, for each external agency with which the department can share such data, including, but not limited to, the length of time such agencies may retain such data, any restrictions on the purposes for which such data can be used, the format and method in which the data will be provided, and what, if any, anonymization methods and/or redactions will be applied to the data prior to its dissemination.

4. The department shall include in each impact and use policy the potential disparate impacts on protected groups of the use and deployment of the surveillance technology itself, including, but not limited to, any variation in the accuracy of said technology on the basis of a characteristic protected by New York City Human Rights Laws.

5. The department shall revise the Health & Safety Reporting sections of all published impact and use policies, to include any safety hazards that are identifiable on the basis of existing research, manufacturer warnings, or evaluations by experts in the field, or to state that no such hazards have been identified after a search for relevant information.

6. Within 180 days of the effective date of this paragraph, the department shall create an internal tracking system for every instance in which the department provides an external agency with data collected via surveillance technologies that the department controls, including the name of the agency, the date the data was provided, and a detailed description of the information that the provided data contained.

7. In order to facilitate the department of investigation's audit requirements pursuant to subdivision c-1 of section 803 of New York city charter, the department shall:

a. provide the department of investigation, within 90 days of the effective date of this paragraph, with information indicating, for each surveillance technology, the various types of data collected and which department units maintain that information. The department shall include information about the retention procedures and practices for each type of data collected so that the department of investigation can assess the department's compliance with the impact and use policies.

b. provide the department of investigation with any data access and retention policies that are included in the existing contracts with vendors who supply the surveillance technologies used by the department.

c. provide the department of investigation with the data access and retention policies contained in any newly executed contracts with surveillance technology vendors by

the 15th of each quarter (i.e., January, April, July, and October).

d. provide the department of investigation, within 30 days of the effective date of this paragraph, an itemized list of the surveillance technologies that it uses. This list should include information concerning the functionalities of each technology, so that the department of investigation can assess whether the department has, in fact, issued an impact and use policy that covers each surveillance technology that has a distinct functionality or capability.

e. provide the department of investigation with quarterly updates, beginning January 15, 2024, reflecting newly acquired or discontinued technologies in an itemized list of the surveillance technologies that it uses. Thereafter, updates should be made available by the 15th of each quarter (i.e., January, April, July, and October).

8. The department shall issue a press release announcing the publication, related public comment period of any new impact and use policies, and subsequently publish the press release on its website.

Many of these electronic surveillance tools should not be used at all, but some have an elevated concern based upon the NYPD's reliance on them, 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. Regarding facial recognition technology, The Legal Aid Society believes its use by the NYPD should be banned. As discussed in more detail above in section IV(D)(1), there is no amount of transparency or oversight which will allow for the use of facial recognition by the NYPD in a way that is not bias, lead to false arrests, or cause significant harm to individuals and communities. Similarly, as discussed in section IV(D) (2-3), we continue our call to ban the Criminal Groups Database (aka Gang Database).

VII. CONCLUSION

The passing of the POST Act had admirable intentions, but the NYPD has chosen to “comply” in ways that mostly 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 small step in the right direction. The Legal Aid Society encourages the City Council to enact into law the changes we have endorsed here.

Statement by P. A. Carroll

As a voter in District 3 (CM Erik Bottcher) who has also lived in District 26 (CM Julie Won) and elsewhere in the boroughs, I am glad to submit testimony on legislation impacting all New Yorkers. As a very longtime Amnesty International member, I agree that it is crucial to clarify and strengthen the 2020 POST Act, as NYPD has not been fully cooperative or accountable on the new surveillance technologies it is using. Thank you to Council Members Julie Won, Christopher Marte and Amanda Farias for introducing and supporting the proposed laws 1193-2023 and 1207-2023; I hope the Committee will approve them and that there will be solid support for them in the entire Council. Following, I will make some personal remarks:

This is common-sense legislation that would guard against abuses. While like anyone who has been a victim of a crime, I appreciate the role of police officers, especially those who are professional and attentive. However, most New Yorkers are aware of abuses ranging from officers who simply don't do their jobs to officers who lie or engage in criminal activities. Moreover, some NYPD policies are unjust or inadvertently lead to problematic situations.

As a New Yorker active in public service after 9/11, I assisted scores of Muslim immigrant families with the breadwinner rounded up and jailed due to reactionary "war on terror" over-reaction. None were terrorists, even though the stigma of their arrest (and eventual deportation) remained. Over 75 were placed in solitary confinement for many months on end. City, State and Federal levels of government created new problems while confronting others.

During that period after the terror attacks it became clear that due to my humanitarian work in the NYC Muslim community I was under some sort of surveillance –besides hearing clicks on my phone, I received a warning to me left anonymously on my home answering machine. When I submitted a form to the NYPD regarding any possible file, they declined to share any data. This did not greatly concern me, but it left me with a perspective that more vulnerable New Yorkers certainly share. What will happen to all the data that the department gathers, and who has access? How to challenge wrong information?

At annual community meetings with Police Commissioner Kelly, I recall asking him simple questions, such as how many undercover officers there were—which he refused to answer. Then, approximately five years after 9/11 I joined Muslim leaders and activists [to criticize NYPD policies to surveil Muslim businesses](#), mosques and communities, and the simplistic analysis used to identify "radicalism." There was quite a lot of resistance to our constructive criticism from police officials and even Mayor Bloomberg. But the policies were simply not well informed and alienated whole communities. And this was before the development of the much more intrusive technologies that are under discussion today.

In more recent years I have worked with a nonprofit that raises awareness concerning the protection of minority communities primarily in China, India and Burma (Myanmar). Our lawyer for a lawsuit against the military government of Myanmar in 2026 was a [Sikh Indian man](#) who recently [made the news](#) because the Government of India had organized a plot to murder him on

US soil. Our efforts and those of our progressive Hindu allies have been distorted in social media by shadowy organizations like “Disinfo Lab” associated with Indian government intelligence services, and I have even been listed as a minor player on its misleading affinity maps. This week the Washington Post [described how](#) Disinfo Lab shared false claims with US elected officials, who then forwarded them onto law enforcement. Will these referrals lead to surveillance? What are the rules?

Now with a period of social tension due to Israel’s war on Hamas, and its impact on Palestinian civilians both in Gaza and in the occupied West Bank, the organizations I have worked with may fall under greater scrutiny once more. Already, valid concerns about Antisemitism have been distorted and manipulated to silence criticism of disproportionate military response by the Israeli policies. Insensitive comments are conflated with “hate.” What impact might this political climate have this on surveillance policies, including at the NYPD?

Given the NYPD’s long track record of evading and minimizing oversight, the two proposed laws under discussion today will help ensure the checks and balances of our democracy continue to function in this era of increasing reliance on expensive and often intrusive technology (including but not limited to drones, robots, keyword and biometric surveillance and even artificial intelligence). While some of these technological tools may be useful in very specific situations, abuses do occur, and it is better to prevent problems rather than to continue to deal with the divisive and sometimes tragic social impact.

As per “Int 1193 2023”, introduced by CM Amanda Farias, the NYPD should indeed supply the Department of Investigation (DOI) with an itemized list of all surveillance technologies currently used by the Department, and provide information on relevant data access and retention policies. NYPD should provide DOI with quarterly updates on surveillance technologies, policies and contracts. There is nothing in this that would inhibit policing or interfere with specific investigations.

On the contrary, the Department cannot do its work without public trust. Trust is in very short supply. Therefore, transparency matters. As per the proposed legislation (Int 1207-2023) introduced by CM Julie Won, NYPD should publish “Impact and Use” policies for each individual surveillance technology used by the Department, identifying any “external entities” that receive data. It is also important to see its evaluation of potentially disparate impacts on protected groups arising from using such technologies. We are already aware that certain communities are much more likely to be surveilled. How will the disparate impact be managed or minimized?

Many questions remain. But at least, more oversight will lead to an accountable department, along with more community trust, and therefore more effective policies for a safer New York.

P. “Adem” Carroll 12/15/2023

FOR THE RECORD

FOR THE RECORD

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

_____ x

Index Number:
101048-2023

Towaki Komatsu,
Petitioner,

**AFFIDAVIT IN
SUPPORT**

-against-

The City of New York, Martha Calhoun, Molly Park,
Ann Marie Scalia, Vincent Pullo, Samuel, Spitzberg,
Nigel Marks, Steven Banks, Edward Cyrus, Jeffrey
Mosczyk, Marin Gerber, Urban Pathways, Inc.,
Kristen Benjamin-Solis, Lisa Lombardi,

(all individuals listed above are being sued in their
individual and current capacities as well as their
former capacities in certain instances as described
later in this petition)

Respondents,

_____ x

STATE OF NEW YORK)
COUNTY OF NEW YORK) ss:

Towaki Komatsu, being duly sworn, deposes and says:

1. I am the petitioner in this case and make this affidavit in support of the attached
emergency order to show cause application. This affidavit is comprised of the following sections:

<u>Section</u>	<u>Page</u>
Preliminary Remarks	2
Relief Sought.....	2
Why This OSC is an Emergency OSC.....	2
Relevant Legal Standards.....	7

FOR THE RECORD

FOR THE RECORD

Vaughan to let me keep that original order. Judge Frank was in his courtroom through the entire time that I interacted with Mr. Vaughan on 4/9/19 while I lawfully directed Mr. Vaughan to hand me back Judge Frank's original 4/9/19 order that confirmed that he (Judge Franks) had marked the "Case Disposed" box in that order to illegally dismiss K1 then.

5. On page 2 and in numbered paragraph 2 in 6/19/19 reply affirmation that Ms. Yogiaveetil filed in K1, she expressed that Judge Bannon's 8/10/17 decision in K1 severed claims of mine in K1 that included a claim that she (Ms. Yogiaveetil) stated was about HRA having unlawfully precluded me from attending certain public meetings. Ms. Yogiaveetil fraudulently and prejudicially didn't acknowledge the critically significant fact that that claim was about and against personnel of multiple government agencies that partly consisted of the NYPD. That confirms that that claim wasn't limited to HRA. Contrary to Ms. Yogiaveetil's lies, Judge Bannon's explicitly stated the following on page 2 in her 8/10/17 decision before she then stated in the same paragraph that that claim was actually about my having been unlawfully precluded from public meetings of municipal agencies in violation of my constitutional rights:

"The petition/complaint also seeks money damages and / or injunctive relief against the HRA **and several other municipal agencies and their employees**"

(boldface and underline formatting added for emphasis)

6. Before SCOTUS stated in Roman Catholic Diocese of Brooklyn v. Cuomo, 141 S. Ct. 63, 592 U.S., 208 L. Ed. 2d 206 (2020) that "such remote viewing is not the same as personal attendance" and though Ms. Yogiaveetil stated the following between the bottom and top of pages 21 and 22 in her 6/19/19 reply affirmation, e-mail evidence in the 2/1/21 discovery material implicated Steven Banks and Jacqueline Bray while they worked for HRA about decisions that were made on or about 4/11/17 by senior HRA personnel (including Raquel Lucas while she then worked for Mr. Banks as an assistant) to partner with personnel who then worked

partly for the NYPD, CAU, and Mayor's Office to illegally and on a continuous basis a) prevent me on from lawfully attending public meetings that were public forums that members of the public conducted partly with City and State of New York government personnel and censors in journalism in 2017 in New York City and b) otherwise intentionally and pre-emptively restrict my ability to observe such public forums in the buildings in which they were conducted from overflow rooms while illegally discriminating against me by subjecting me to illegal segregation in flagrant violation partly of my First and Fourteenth Amendment rights:

"Plaintiff argues that he received a FOIL response from the Mayor's Office- which he does not attach and of which Your Affiant is not in possession-that supports his claims that HRA prevented him from attending public meetings or hearings. In the absence of these records, HRA cannot properly respond to Plaintiff's allegations. Plaintiff has not submitted any proof in admissible form demonstrating that HRA was involved in any decision to exclude him from the Town Hall meeting. His arguments concern the purported actions of individuals who are not employees or agents of the HRA."

7. Findings from the Second Circuit's 10/27/23 order in Network Data Rooms, LLC v. Saulrealism LLC, No. 22-3226 (2d Cir. Oct. 27, 2023) that I presented in this affidavit's "Relevant Legal Standards" section reject what Ms. Yogiaveetil stated in the preceding excerpt about whether those who prevented me from lawfully attending public meetings that were public forums in New York City in 2017 in the rooms in which they were conducted were agents of HRA for that purpose.

8. The e-mail shown next is about K1 and I and is from a PDF file that I received on 2/15/19 from the Mayor's Office in response to a FOIL demand that I submitted to it. That PDF file is hereinafter referred to as "the 2/15/19 PDF file". This e-mail that was sent by Jaclyn Rothenberg on 6/28/17 at 5:18 pm confirms that while she then worked for the Mayor's Office, she was in violation of Judge Ostrager's 1/17/17 sealing order in K1 that sealed K1 and authorized me to proceed anonymously in K1. That sealing order prohibited those who didn't

work for HRA, weren't me, and otherwise weren't personnel of the UCS to have access to information about K1 while it was sealed. This e-mail confirms that Ms. Rothenberg also illegally communicated information about K1 to others while K1 was then sealed.

From: Rothenberg, Jaclyn
Sent: Wednesday, June 28, 2017 17:18
To: Ramos, Jessica
Cc: Phillips, Eric; Redmond, Howard DI.; Hagelgans, Andrea; Casca, Michael; Arslanian, Kayla; Carrion, Marco A.; Wolfe, Emma
Subject: RE: town halls

Confirmed that he appeared at 4WTC on June 6 and served an Order to Show Cause. That OSC and another pending matter were submitted to the court for a decision on June 7. HRA is still waiting for the written decision.

9. The e-mail shown next is also about K1 and I and from "the 2/15/19 PDF file. That e-mail was sent on 6/28/17 at 5:42 pm by New York State Senator Jessica Ramos while she then also worked for the Mayor's Office. She sent that e-mail to a censor in journalism named Erin Durkin while Ms. Durkin then worked for the New York Daily News. Her remarks in that e-mail also confirm that she was in violation of Judge Ostrager's 1/17/17 sealing order in K1. This e-mail confirms that Ms. Ramos also illegally communicated information about K1 to others while K1 was then sealed.

On Wed, Jun 28, 2017 at 5:42 PM, Ramos, Jessica
<JRamos@cityhall.nyc.gov> wrote:

Mr. Komatsu wanted a storage allowance, for which he was ineligible because he had an apartment. We also referred him to multiple legal services providers about this specifically and all of them denied him.

Mr. Komatsu has been served an Order to Show Cause due to his appearance at HRA in June, when he showed disruptive behavior. That OSC and another pending matter were submitted to the court for a decision on June 7. HRA is still waiting for the written decision.

Sent from my BlackBerry 10 smartphone.

10. The e-mail shown next is part of the 2/1/21 discovery material, was sent by Raquel Lucas to personnel of HRA and the Mayor's Office while she then worked for Steven Banks as an assistant, and incriminates her as well as Mr. Banks and Jacqueline ("Jackie") Bray in regards to their efforts to illegally prevent me from lawfully attending a public town hall meeting on 4/13/17 while Ms. Lucas lied about me in that e-mail by fraudulently claiming that a) I had harassed Mr. Banks instead of acknowledging that the opposite was true partly when Mr. Banks lied to my face on 4/11/17 in Staten Island about why I hadn't been provided legal assistance as a result of HRA's efforts, b) a safety concern about me existed, c) I had been disruptive, and d) HRA had tried to help me instead of harm me partly by criminally stealing my originally scheduled 4/12/17 oral arguments hearing in K1 through illegal *ex-parte* communications with

Judge Bannon and subjecting me to the B&S.

From: Lucas, Raquel [mailto:quezadar@hra.nyc.gov]
Sent: Thursday, April 13, 2017 9:40 AM
To: Lauter, Rachel; Arslanian, Kayla; Gillroy, Elizabeth
Cc: Bray, Jackie
Subject: Townhall Tonight Re: Towaki Komatsu

+Elizabeth and Jackie

Good Morning,

Jackie Bray had spoken to the Commissioner this morning about this client Towaki Komatsu who has been extremely disruptive at events with the Mayor and Commissioner Banks. His case history is below. His behavior has been borderline harassment to the Commissioner, and he is increasingly belligerent despite our best efforts to assist him. Is there any way without making a scene to not allow him in the town hall tonight from a safety perspective? Jackie Bray and I are both around if you want to talk further. Thanks.

11. The e-mail about me shown next is also part of the 2/1/21 discovery material and was sent on 4/13/17 at 5:13 pm by Howard Redmond while he was then the head of the NYPD security detail for Bill de Blasio while Mr. de Blasio was New York City's Mayor. He sent that e-mail to Jerry Ioveno while Mr. Ioveno also was a member of that NYPD security detail. Mr. Redmond's remarks in that e-mail were in response to Raquel Lucas' request for me to be illegally barred from attending a public town hall meeting on 4/13/17 in Staten Island that I never intended to attend and never told anyone nor otherwise suggested that I would attend. Mr. Redmond confirmed in this e-mail that he and others would illegally attempt to prevent me from attending that town hall meeting at the request of Raquel Lucas of HRA before Mr. Redmond resumed that illegal practice as a continuing violation on 4/27/17 by criminally preventing me from lawfully attending a public town hall meeting in Long Island City in Queens.

From: REDMOND, HOWARD
Sent: Thursday, April 13, 2017 5:13 PM
To: loveno, J
Subject: Jerry see below

Towaki Komatsu has been extremely disruptive at events with the Mayor and Commissioner Banks. His case history is below. His behavior has been borderline harassment to the Commissioner, and he is increasingly belligerent despite our best efforts to assist him. Is there any way without making a scene to not allow him in the town hall tonight from a safety perspective.

If this guy shows up alert Cityhall Staff do not let him in. Worst case we will put him in overflow.

Sent from my BlackBerry 10 smartphone on the Verizon Wireless 4G LTE network.

12. The e-mail about me shown next also is part of the 2/1/21 discovery material and was sent on 4/13/17 at 1:58 pm by Jeff Lynch while he worked for the CAU. He sent that e-mail to senior personnel of HRA and the Mayor's Office as he confirmed that he was among criminal accomplices of HRA in attempting to illegally prevent me from attending a public town hall meeting on 4/13/17 in Staten Island.

From: Lynch, Jeff
Sent: Thursday, April 13, 2017 1:58 PM
To: Lauter, Rachel; Lucas, Raquel (HRA); Arslanian, Kayla; Gillroy, Elizabeth
Cc: Bray, Jackie; Carrion, Marco A.; Miller, Harold; Stribula, Shauna
Subject: RE: Townhall Tonight Re: Towaki Komatsu

+ Harold and Shauna

Yes, we alerted HRA about his RSVPing for the Resource Fair, and Harold talked to him when he came in, and outside in the hallway.

He has not RSVPed for tonight's town hall, so if he shows, he will likely be sent to the overflow room. We will also flag for the detail.

13. What appears next are a) the e-mail header section for an e-mail about me that Jaclyn Rothenberg sent on 6/29/17 at 9:43 am while she then worked for the Mayor's Office to other City of New York personnel and b) a relevant excerpt from that e-mail that also is part of the 2/1/21 discovery material.

From: Rothenberg, Jaclyn
Sent: Thursday, June 29, 2017 9:43 AM

To: Ramos, Jessica; Carrion, Marco A.; Da Costa, Ricky
Cc: Hagelgans, Andrea; Phillips, Eric; Redmond, Howard DI.; Casca, Michael;
Arslanian, Kayla; Wolfe, Emma; Lynch, Jeff; Stribula, Shauna
Subject: RE: town halls

He then signed up to come to the SI resource center during CH in Staten Island to see the mayor and was not allowed in because he had already spoken to the mayor in the prior town hall - he then came to the IDNYC mobile outreach vehicle while Nisha and Banks were doing a social media taping - when he said that we should give him a storage allowance because he had just sued us Banks said that he did not think he would win his case and he became very angry and stormed off saying that he would go to the press.

14. The preceding excerpt from that e-mail confirms that Ms. Rothenberg confirmed that I was barred from attending a public resource fair meeting that was a public forum that was held on 4/11/17 in Staten Island. The fact that I had previously attending a town hall meeting on 3/15/17 that members of the public held with Mr. de Blasio and others wasn't valid legal grounds to bar me from the 4/11/17. However, Harold Miller³ and members of Mr. de Blasio's NYPD security detail illegally wouldn't let me enter the room in which that public forum was held in Borough Hall on 4/11/17 after I entered that building to do so while that public forum was still being held. That occurred after I registered in advance with the Mayor's Office to lawfully attend that public meeting and travelled all of the way from the Bronx to Staten Island on 4/11/17 for that specific purpose. Contrary to some of Ms. Rothenberg's remarks about me in the preceding excerpt, the following is true:

a. I wasn't allowed to lawfully attend the 4/11/17 public resource fair mainly because Mr. Banks panicked while talking with me on a sidewalk near Borough Hall in Staten Island on 4/11/17 while that resource fair meeting was being held nearby. He panicked in response to my having told him that I intended to talk with Mr. de Blasio during that public resource fair meeting about the fact that he (Mr. Banks) had just lied to me again while I talked

³ Mr. Miller then worked for the CAU.

with him on that sidewalk.

b. Contrary to Ms. Rothenberg's claim, I talked with Mr. Banks on a sidewalk in Staten Island before I attempted to enter the Borough Hall building nearby. Also, I didn't tell Mr. Banks that HRA needed to provide me benefits for storage unit rental expenses because I had sued HRA. I instead told him that because I was both eligible and entitled as a matter of law to that benefit.

c. I was angry while I talked with Mr. Banks on 4/11/17 partly because I already knew before I talked with Mr. Banks on 4/11/17 that Judge Bannon and Jeffrey Mosczyk of HRA illegally and jointly a) stole my scheduled 4/12/17 oral arguments hearing in K1 by engaging in illegal *ex-parte* communications and b) further discriminated against me by doing so on account of the material fact that I'm Jewish and Mr. Mosczyk premised his 4/5/17 request to Judge Bannon to adjourn the 4/12/17 oral arguments hearing on a claim that he couldn't participate in it on 4/12/17 because that would occur during Passover. Since Judge Bannon scheduled that hearing on 1/26/17, Mr. Mosczyk had ample time prior to 4/11/17 to have a) urged her to reschedule it in a way that would have caused it to be held before or after 4/12/17, b) arranged to have substitute counsel represent HRA during the 4/12/17 hearing, and c) not engaged in illegal and pretextual *ex-parte* communications with Judge Bannon. However, he illegally and prejudicially didn't do so. As I mentioned in my 10/13/23 OSC, Judge Bannon's court clerk (Jerome Noriega) left me a voicemail message at 9:56 am on 4/11/17 and his remarks then enabled me to learn then that Mr. Mosczyk had criminally subjected me to pretextual witness tampering and gamesmanship by stealing my scheduled 4/12/17 oral arguments hearing in K1. He did so while I was scheduled to participate in parallel litigation on 4/11/17 in K4 as a result of a fair hearing that OTDA would conduct then by telephone between HRA and I about a

storage unit rental expense claim of mine that I asserted both in K1 and K4. I had planned on testifying about that claim on 4/12/17 in K1 during oral arguments then while I would have discussed what transpired on 4/11/17 during my OTDA fair hearing about that same matter. I was also angry at Mr. Banks while I talked with him on 4/11/17 in response to him having lied to my face yet again then about why I hadn't been provided legal assistance from business partners of HRA that HRA referred me to.

d. When I abruptly ended my conversation with Mr. Banks on 4/11/17, I told him that I was done talking with him and that I intended to talk with Mr. de Blasio about him while attending the 4/11/17 public resource fair nearby. I didn't tell him that I intended to talk with the press then about that.

15. The following is an e-mail that is part of the 2/1/21 discovery material and Mr. Banks sent on 4/11/17 at 12:48 pm about the interactions that he and I just had on a public sidewalk near Borough Hall in Staten Island:

On Apr 11, 2017, at 12:48 PM, Banks, Steven <banksst@hra.nyc.gov> wrote:

++++ Fyi" he just showed up at the IDNYC Command Center parked by Borough where Nisha and I were doing a stand up for social media that had just finished, was belligerent, tried to tape our conversation and did film me walking away from he - he is headed back into Borough Hall saying he is going to the press.

Sent from my BlackBerry 10 smartphone on the Verizon Wireless 4G LTE network.

16. In the preceding e-mail, Mr. Banks fraudulently omitted the material fact that his lies to my face during my 4/11/17 chat with him were what prompted me to be irritated by him then. He also lied by claiming that I was belligerent. Instead of behaving that way, I simply and abruptly terminated my conversation with him. Also, he lied by saying that I told him that I would contact the press then about my conversation with him. I instead told him that I intended to talk to Mr. de

Blasio about that.

17. The additional e-mails about me that are shown next also are part of the 2/1/21 discovery material and were sent on 6/28/17 mainly by Jaclyn Rothenberg while she worked for the Mayor's Office to other City of New York personnel as she a) partly addressed why I was illegally prevented from attending public meetings that were public forums that City and State of New York government personnel conducted partly with members of the public; b) pretextually lied about me partly by claiming that I was disruptive and threatened security; and c) tied the rationale for the illegal acts and omissions that were perpetrated against me in regards to my ability to lawfully attend public forums to my claims and criticism partly against HRA in K1 pertaining to storage unit rental expense matters:

From: Rothenberg, Jaclyn
Sent: Wednesday, June 28, 2017 17:33
To: Phillips, Eric; Ramos, Jessica
Cc: Redmond, Howard DI.; Hagelgans, Andrea; Casca, Michael; Arslanian, Kayla; Carrion, Marco A.; Wolfe, Emma
Subject: RE: town halls

Important to note that what he wanted was a storage allowance, which we did not allow since he had an apartment. He sued us a couple of times about it. We also referred him to multiple legal services providers about this specifically and all of them denied him.

From: Rothenberg, Jaclyn
Sent: Wednesday, June 28, 2017 17:55
To: Hagelgans, Andrea; Phillips, Eric
Cc: Ramos, Jessica; Redmond, Howard DI.; Casca, Michael; Arslanian, Kayla; Carrion, Marco A.; Wolfe, Emma
Subject: RE: town halls

He has never threatened Steve. He sued HRA.

Only shown disruptive behavior. Believe per below he threatened security.

From: Hagelgans, Andrea
Sent: Wednesday, June 28, 2017 5:42 PM

To: Phillips, Eric; Rothenberg, Jaclyn
Cc: Ramos, Jessica; Redmond, Howard DI.; Casca, Michael; Arslanian, Kayla; Carrion, Marco A.; Wolfe, Emma
Subject: RE: town halls

Why did we use the term "threat" if he didn't?

On Jun 28, 2017, at 5:38 PM, Rothenberg, Jaclyn <JRothenberg@cityhall.nyc.gov> wrote:

The threat was that he was dissatisfied with the outcome of our help. There was no physical violence suit. Though he has shown disruptive behavior.

18. The two e-mails shown next about me also are shown in the 2/1/21 discovery material and were sent on 6/28/17 partly by Marco Carrion while he was the CAU's commissioner as he did the following:

- a. Directly implicated Steven Banks of HRA by confirming that he was the person who was the one who originally "flagged" me in a manner that proximately caused illegal acts and omissions to be committed against me by City and State of New York government personnel concerning my ability to lawfully attend public meetings that were public forums that were conducted in 2017.
- b. Lied by fraudulently claiming that a) I had been disruptive and engaged in a tirade and b) HRA had attempted to assist me.
- c. HRA couldn't do anything to assist me for what was then a current legal case of mine that included K1.

On Jun 28, 2017, at 2:12 PM, Carrion, Marco A. <mcarrion@cityhall.nyc.gov> wrote:

He was originally flagged by Steve Banks. They have attempted to assist him numerous times but there is nothing they can do for his current legal case. He has since shown up to HRA and been disruptive. He did show up to the Chelsea townhall where he was called on and asked a question (and went on a long tirade re: Banks).

From: Carrion, Marco A.
Sent: Wednesday, June 28, 2017 19:16
To: Da Costa, Ricky
Cc: Ramos, Jessica; Rothenberg, Jaclyn; Hagelgans, Andrea; Phillips, Eric; Redmond, Howard DI.; Casca, Michael; Arslanian, Kayla; Wolfe, Emma; Lynch, Jeff; Stribula, Shauna
Subject: Re: town halls

HRA flagged him to us as someone who was disruptive and who was/is harassing Banks.

What is the question for CAU?

19. The e-mail shown next is one that I automatically received at 10/31/23 at 11:20 pm from Lisa Fitzpatrick who had been working for HRA as its administrator before her remarks in this e-mail revealed that Scott French took over that job on 10/28/23:

From: Fitzpatrick, Lisa <fitzpatrickl@hra.nyc.gov>
Sent: Tuesday, October 31, 2023 11:20 PM
To: Towaki Komatsu <towaki_komatsu@yahoo.com>
Subject: Automatic reply: [EXTERNAL] Re: Problems by HRA with enabling me to recertify for SNAP benefits today prior to a deadline

Thank you for your email. Scott French is the HRA Administrator as of 10/28/23. Please email Mr. French directly or call 929.221.6194 for assistance.

20. Prior to receiving that e-mail, Mr. French worked for HRA as Mr. Banks' Chief of Staff while Mr. Banks was HRA's commissioner. While he held that earlier job, Mr. French sent the following e-mail about me on 10/25/17 at 8:54 am partly to Mr. Banks in connection with a joint effort and conspiracy by him and other senior personnel of HRA, the CAU, the NYPD security detail for Bill de Blasio while he was New York City's Mayor, and personnel of the Mayor's Office to illegally prevent me from attending a public resource fair meeting that was held on 10/25/17 in Brooklyn:

From: "French, Scott" <frenchs@hra.nyc.gov>
Date: October 25, 2017 at 8:54:48 AM EDT

To: "Haley, Molly (MHaley@cityhall.nyc.gov)" <MHaley@cityhall.nyc.gov>.
"Lauter, Rachel" <rlauter@cityhall.nyc.gov>.
"mcarrion@cityhall.nyc.gov" <mcarrion@cityhall.nyc.gov>
Cc: "Banks, Steven" <banksst@hra.nyc.gov>
Subject: Resource FAiur

Hi Rachel, Molly and Commissioner Carrion -

I just wanted to make you aware that Mr. Komatsu, who has attended several events where the Mayor and Commissioner Banks are in attendance, indicated at a Access to Counsel Town Hall last night that CM Levine and CM Perkins held that he was planning on attending today's Resource Fair and expected that he wouldn't be allowed in to the Fair.

Wanted to flag for you so you could let Redmond know (who is very familiar with Mr. Komatsu). He may ultimately not show up but wanted to flag as a possibility.

Thanks
Scott

Scott French | *Chief of Staff*
Office of the Commissioner
150 Greenwich St. Floor 42, New York, NY 10007
T: 929-221-7371
frenchs@hra.nyc.gov | NYC.gov/dss

21. Due to the illegal joint effort and conspiracy that I just discussed, former NYPD Inspector Howard Redmond and other members of the NYPD security for Mr. de Blasio illegally and premeditatively prevented me mainly at the behest of HRA personnel from attending the 10/25/17 public resource fair meeting that was discussed in the preceding e-mail. The fact that Mr. French opted to be involved on 10/25/17 in the illegal scheme and conspiracy that resulted in my illegal exclusion from the 10/25/17 public resource fair meeting in Brooklyn coupled with the fact that HRA personnel continue to illegally prevent me from being able to visit HRA's HQ partly to exercise my First and Fourteenth Amendment right to lawfully examine proposed contracts between HRA and various vendors prior to public hearings about those contracts during which testimony from the public is allowed sufficiently confirms that the continuing

violation doctrine applies to every single public meeting about which I was illegally prevented from attending and was otherwise restricted to observing from an overflow room while I would have otherwise been able to attend those meetings from within the specific room in which they were conducted. This means that equitable tolling is applicable to all such claims of mine. Also, the point that I just made is buttressed by the following additional facts:

a. On 5/12/22, I recorded a video recording with my cell phone at 11:05 am while standing near the entrance to City Hall by Park Row as NYPD Sergeant Ryan Dwyer was among NYPD personnel who criminally prevented me from attending a public hearing that Mayor Adams held inside of the Blue Room in City Hall that I sought to lawfully attend and testify in.

A copy of that video recording is available at

[https://drive.google.com/file/d/11ECImMQCpLOZzGA2A0xU2vdYzW-](https://drive.google.com/file/d/11ECImMQCpLOZzGA2A0xU2vdYzW-bLTb6/view?usp=sharing)

[bLTb6/view?usp=sharing](https://drive.google.com/file/d/11ECImMQCpLOZzGA2A0xU2vdYzW-bLTb6/view?usp=sharing). Testimony from the general public was allowed during that public forum and Mr. Dwyer then worked for the NYPD security detail for Mayor Adams. NYPD Inspector Howard Redmond was at one point Mr. Dwyer's supervisor for that NYPD security detail.

b. On 11/16/21, I recorded a video recording with my cell phone at 5:19 pm while attending a public resource fair meeting that members of the public conducted partly with Mr. de Blasio while he then was New York City Mayor, Eric Adams, and others at 240 Nassau Street in Brooklyn. A copy of that video recording is available at

https://drive.google.com/file/d/11wYrY8we5z5iTuSNzRjH5S6bi0f59f_4/view?usp=sharing.

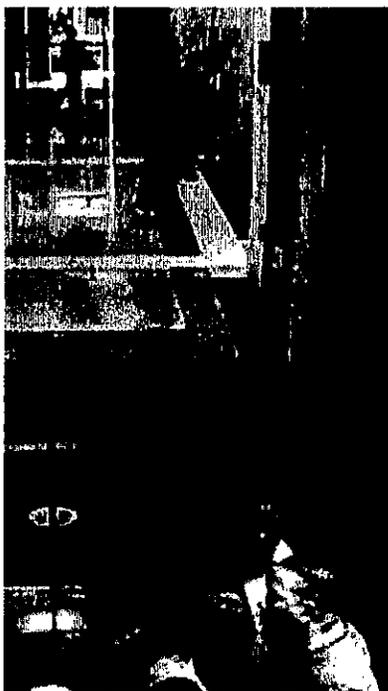
What is shown and heard in that video confirms that after I talked with Mr. de Blasio during that meeting at the elapsed time of 4 seconds. Joni Kletter and Pinny Ringel illegally and jointly prevented me between the elapsed times of 1 minute and 4 seconds and 1 minute and 30 seconds

from having a conversation with Steven Banks then while he was then HRA's commissioner, Mr. Ringel worked for the CAU, and Ms. Kletter was an attorney and the commissioner of New York City's Office of Administrative Trials and Hearings. Ms. Kletter is heard in that video as she identified herself at the elapsed time of 35 seconds. She explained to me at the elapsed time of 1 minute and 18 seconds that the reason why I couldn't talk with Mr. Banks then was due to litigation of mine. However, my conversation with him then didn't necessarily need to be about that and I pointed that out to her. She and Mr. Ringel illegally prevented me from talking with Mr. Banks then partly about job opportunities for me with HRA shortly after I talked with Mr. de Blasio about that. This confirms that Mr. Ringel and Ms. Kletter illegally violated findings in *Board of Regents of State Colleges v. Roth*, 408 U.S. 564, 92 S. Ct. 2701, 33 L. Ed. 2d 548 (1972) that among other things, confirms that Fourteenth Amendment liberty rights include the right to engage in the common occupations of life.

c. On 9/23/21, I recorded a video recording with my cell phone at 1:46 pm while attending a public resource fair meeting that members of the public conducted partly with Mr. de Blasio and Mr. Banks in Kew Gardens's Borough Hall building in Queens. A copy of that video recording is available at <https://drive.google.com/file/d/1yuaEKbRsaYZ-80K1gHngjK3r8rvdUjwe/view?usp=sharing>. What is shown and heard in that video at the elapsed time of 31 seconds confirms that Mr. Banks told me that he wouldn't talk with me then because I had commenced litigation that he claimed was threatening as he also fraudulently mischaracterized e-mails that I sent to him as being threatening. He also illegally tried to coerce me to step further away from him than I then was in spite of the fact that meeting was a public forum and I was standing roughly 5 feet away from him. That violated my First and Fourteenth Amendment rights. The only threatening aspect of such litigation and e-mails was that he stood

to lose in such litigation and I informed him about that in e-mails that I sent to him to courteously let him know that he didn't have a valid defense in such litigation. The fact that his rationale for discriminating against me during that public meeting compared to other members of the public who also attended it was partly due to litigation that I commenced partly against him and HRA confirms that his treatment of me then was a continuing violation that related back to claims that I asserted in K1 and K5 that were partly about the fact that I was illegally prevented from attending public meetings in April and May of 2017 by City of New York personnel.

22. Before Judge Schofield pretextually and fraudulently dismissed K5 on 9/27/21 as an act of First Amendment retaliation against me, she illegally enabled me to be criminally assaulted and otherwise illegally seized and harassed repeatedly inside of DPM by CSOs. For example, federal court security officer Ralph Morales criminally assaulted me inside of DPM on 8/8/18 and lied about that by claiming that I tried to assault him then. He lied about that just one day after a video security camera that the USMS controls recorded him inside of DPM on its first floor as he illegally stalked and harassed me while also sticking one of his fingers in very close proximity to my face. This is shown in the following screenshot from that video:



23. . That occurred while he was off-duty as a CSO and other CSOs were nearby and illegally didn't intervene on my behalf against him. Due to Mr. Morales' lies about me about my interactions with him on 8/8/18 inside of DPM, I was maliciously prosecuted in K7 before that case was dismissed on 10/21/19 by Judge Tiscione at the request of Sarah Mortazavi of the USAO. Neither she nor any other judge has since done anything to end ongoing and unduly prejudicial harassment of me inside of federal courthouses in Manhattan by CSOs and the USMS in furtherance of a vendetta that seems to be fueled by the material fact that I legally whipped CSOs, the USAO, and the USMS as a result of the dismissal of K7. An image of my face and my name is shown on a tablet computer screen inside of DPM in a public area on its first floor as well as on two such screens in security screening areas inside of TM. Those displays are clearly viewable by jurors, potential jurors, witnesses, journalists, attorneys, and others. That confirms that my right to a full and fair hearing and a fair trial has continuously been sabotaged inside of those courthouses since 2018. The preceding discussion is relevant largely because it serves to

dispel any misconceptions that this Court might otherwise have by erroneously thinking that I was properly accorded my First and Fourteenth Amendment right to a fair trial in K5.

24. Moreover, Judge Schofield subjected me to obstruction of justice in K5 while she perpetrated fraud on the court by corruptly, subversively, and prejudicially refusing to allow material evidence that included the following that proved that I was entitled to immediate partial summary judgment in K5 from being considered by her in K5 as her 3/26/21 order (Dkt. 530) in K5 confirms this:

a. Audio recordings that the CCRB provided to me on 3/19/21 that a) I timely apprised Judge Schofield about on 3/26/21 in K5 and b) the CCRB recorded partly of interviews that it conducted partly of former NYPD Inspector Howard Redmond on 8/18/17 and 11/6/17 in response to complaints that I reported to the CCRB partly against him that concerned illegal acts and omissions by City and State of New York government personnel that proximately caused me to be illegally prevented from lawfully attending public meetings in 2017 on many different dates and locations since April of 2017 while they were public forums and otherwise additionally discriminated against and physically assaulted while I lawfully attempted to attend them. The CCRB provided me those audio recordings following the repeal of New York State Civil Rights law 50-a that had previously prohibited the CCRB from providing them to me. The CCRB's audio recording of its 8/18/17 of Mr. Redmond about me is available at <https://drive.google.com/file/d/1bdvEzSznI-m4zg0hzkXMTCGDjO2Ox37g/view?usp=sharing> and its 11/6/17 interview of him about me is available at https://drive.google.com/file/d/1olrXB6qOp4fuotLoCG6xybTi_6b_pXFF/view?usp=sharing. Mr. Redmond is heard in the 8/18/17 audio recording at the elapsed time of 8 minutes and 16 seconds as he stated that a woman with 8 students with her on 4/27/17 at the site of the town hall

meeting in Long Island City in Queens that Mr. Redmond and others illegally prevented me from lawfully attending told him then that he was making her nervous. When she told him that, she did so after I met her outside of and near the school that hosted that public meeting as I informed her that Mr. Redmond was violating my rights to lawfully attend that public meeting for which I had registered in advance with the Mayor's Office to lawfully attend. Mr. Redmond is heard in the 11/6/17 audio recording at the elapsed time of 11 minutes and 30 seconds as he stated the following about me while he didn't elaborate about his remark to identify specific people to whom he was then referring by his reference to "City Hall":

"He's banned from town halls. He's not allowed in the town halls as per City Hall."

b. Highly incriminating e-mail evidence that exists in a 374-page PDF file that I received from the Mayor's Office on 2/15/19 in response to a FOIL demand that I promptly thereafter apprised Judge Schofield about in K5. Information in that PDF file entitled me to partial summary judgment for claims that I asserted in both K1 and K5 that were about illegal act and omission that were perpetrated against me in relation to my efforts to lawfully attend public meetings that were public forums. Such e-mail evidence in that PDF file was a much smaller subset of e-mail evidence that exists in the 2/1/21 discovery material.

c. Relevant excerpts from the New York State Court Officers Rules and Procedures Manual that a) govern how such court officers are required to operate, b) OCA provided to me on 6/30/21 in response to a FOIL demand that I submitted to it, and c) I timely apprised Judge Schofield about on 6/30/21 through a letter that I filed then in K5.

d. The Unusual Occurrence Report that a) was assigned the report number of 75089 (this appears as the first exhibit within the annexed Exhibit A); b) OCA provided to me on 8/28/20 in response to a FOIL demand that I submitted to it; c) was jointly prepared on 5/24/17

by New York State court officers Anthony Manzi, Matthew Brunner, and Ramon Dominguez; d) about their interactions on 5/23/17 inside of the BSC with me, Howard Redmond and other members of the NYPD security detail for Bill de Blasio, and personnel of the Mayor's Office in relation to a public resource fair meeting that was held there then that I attempted to lawfully attend after I registered in advance with the Mayor's Office to do so. I apprised Judge Schofield about that report on 8/28/20 through a letter that I filed then in K5 before she issued an order on 9/10/20 in K5 that confirms that she fraudulently refused to consider that report in spite of the material fact that those who prepared it directly and explicitly implicated both that NYPD security detail and personnel of the Mayor's Office as being the culprits for why I was illegally prevented from lawfully attending the 5/23/17 public resource fair inside of the BSC. The NYAG represented New York State court officers Anthony Manzi, Ramon Dominguez, and Matthew Brunner in K5 while they were defendants in K5. Although an attorney named Monica Hanna was legally required while she then worked for the NYAG to disclose the existence partly to me of the Unusual Occurrence Report that I just discussed in K5 before Judge Schofield issued her 9/30/19 decision in K5, Ms. Hanna prejudicially never did so. The same is true about the New York State Court Officers Rules and Procedures Manual. This confirms that Ms. Hanna perpetrated fraud on the court and obstruction of justice against me in K5 prior to 9/30/19. Moreover, Ms. Hanna fraudulently and prejudicially claimed the following partly on page 2 in the memorandum of law (Dkt. 81) that she filed in K5 on 1/11/19 before Judge Schofield fraudulently and biasedly ignored that these claims by Ms. Hanna were fraudulent and unduly prejudicial to me:

- i. I failed to state a claim in K5 against Mr. Manzi, Mr. Brunner, and Mr. Dominguez on which relief could be granted.

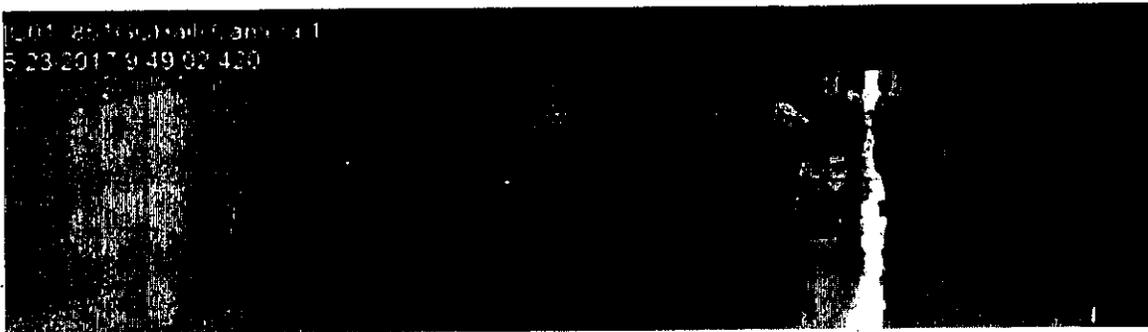
- ii. I didn't adequately allege participation by Mr. Manzi, Mr. Brunner, and Mr. Dominguez in depriving me of constitutional rights of mine on 5/23/17 inside of the BSC.
- iii. Mr. Manzi, Mr. Brunner, and Mr. Dominguez didn't illegally prevent me from engaging in protected speech inside of the BSC on 5/23/17.
- iv. I didn't have any constitutionally protected right to attend the public resource fair meeting that was held on 5/23/17 inside of the VMH.
- v. Mr. Manzi didn't interfere with my possessory interest in any property on 5/23/17 inside of the BSC.

25. The court officers who prepared the Unusual Occurrence Report on 5/24/17 that I discussed above engaged in a criminal cover-up by fraudulently omitting information in that report about the material fact that video recording evidence that I received from OCA that is from video security cameras inside of the BSC and from 5/23/17 confirms that those court officers acted in concert with and as criminal accomplices for the personnel of the City of New York who illegally prevented me from lawfully attending the 5/23/17 public resource fair meeting. Those court officers also lied in that report by fraudulently claiming that I obstructed pedestrian traffic in the BSC and stood near a magnetometer in the BSC after I completed the security screening process to enter the BSC on 5/23/17. Concerning this point, a video recording that OCA provided to me in response to a FOIL demand of mine to it and was recorded on 5/23/17 by a video security camera that OCA controls and was then installed on the first floor in that courthouse is available at

<https://drive.google.com/file/d/1eSnwhc6zHyWrf5JMZ7pZ9cgyUf7USIUw/view?usp=sharing>.

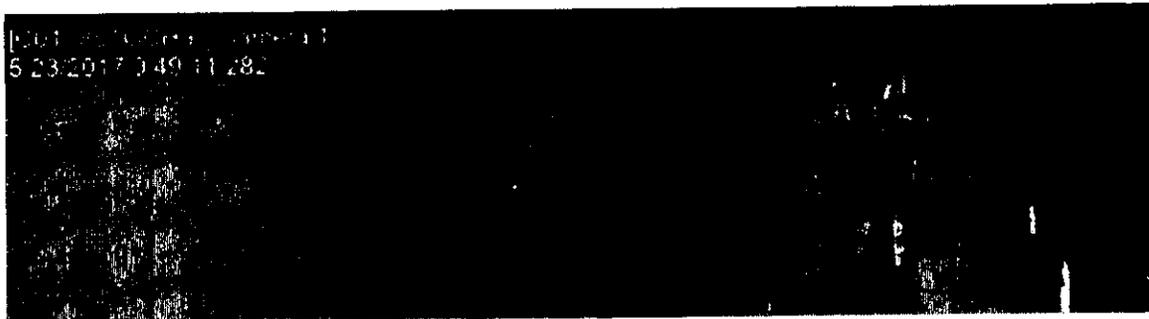
This video is a clip of a longer video recording and this clip shows what was continuously recorded by that camera between 9:19 am and 10:03 am on 5/23/17.

26. The next screenshot is from the elapsed time of 29 minutes and 2 seconds in that video and shows Mr. Manzi while he was illegally trying to coerce me to move further away from a short public corridor located behind him where elevators are located and leads to the VMH in which the 5/23/17 public resource fair was then being held. Mr. Manzi and I are shown next to a table on the left side of the long public hallway that is shown in this screenshot. Jeff Lynch of the CAU is shown here too behind Mr. Manzi as he wore a dark suit and a red tie while court officers Ramon Dominguez and Matthew Brunner stood behind and near Mr. Manzi. A magnetometer device is located more than 10 feet away from where I then stood and is located behind a floor fan that is shown on the right side of this screenshot.



27. The next screenshot is from the elapsed time of 29 minutes and 11 seconds in that video and shows Mr. Manzi as he behaved as a criminal while he flagrantly violated Judge Ostarger's 1/17/17 sealing order in K1 by criminally seizing a large white bag of mine then that contained a copy of my 5/19/17 OSC that I filed in K1 as well as Judge Bannon's 5/22/17 order in response to that OSC. The fact that I immediately seized that bag back from him doesn't change the fact that he criminally tried to coerce me from where I was lawfully then standing as he flagrantly violated my First, Fourth, and Fourteenth Amendment rights then while Mr. Brunner, Mr. Dominguez, and other court officers and members of the NYPD nearby illegally shirked their

legal duty to have promptly and decisively intervened on my behalf against Mr. Manzi then. The woman who is shown at the bottom-left corner in this screenshot then worked for the NYPD and was preoccupied with playing with a cell phone then to perform her legal duty to intervene on my behalf.

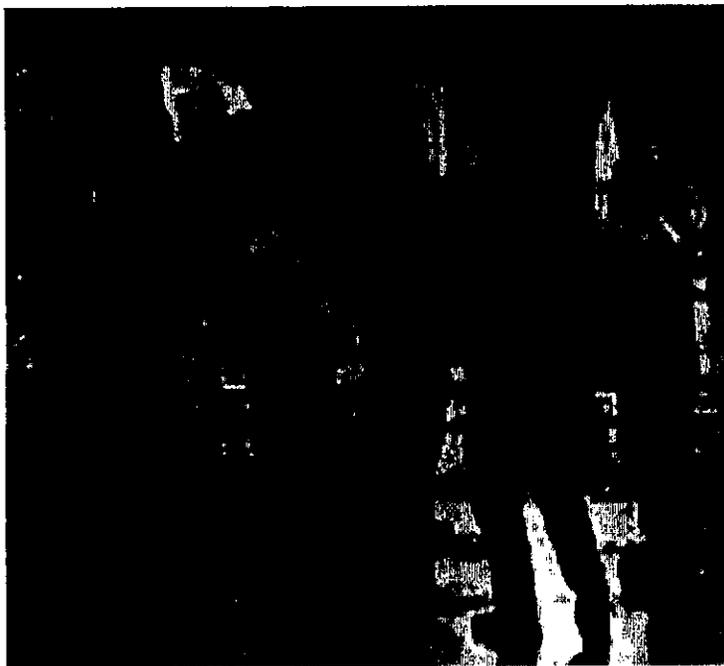


28. The next screenshot is from the elapsed time of 29 minutes and 26 seconds in that video and shows Mr. Manzi as he said "Fuck you" to my face in response to the fact that I lawfully confronted him about having just criminally seized the large white bag of mine and the sealed legal filings that it contained as no one nearby intervened on my behalf then nor thereafter inside of the BSC.

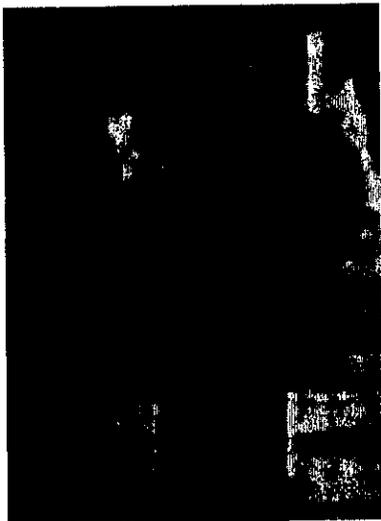


29. The next screenshot is from the elapsed time of 29 minutes and 35 seconds in that video and reflects that the first person who Mr. Manzi walked up to and talked with after he said "Fuck you" to me was NYPD Lieutenant Ralph Nieves while Mr. Nieves was a member of Mr. de

Blasio's NYPD security detail. They appear in the upper-left area in this screenshot.



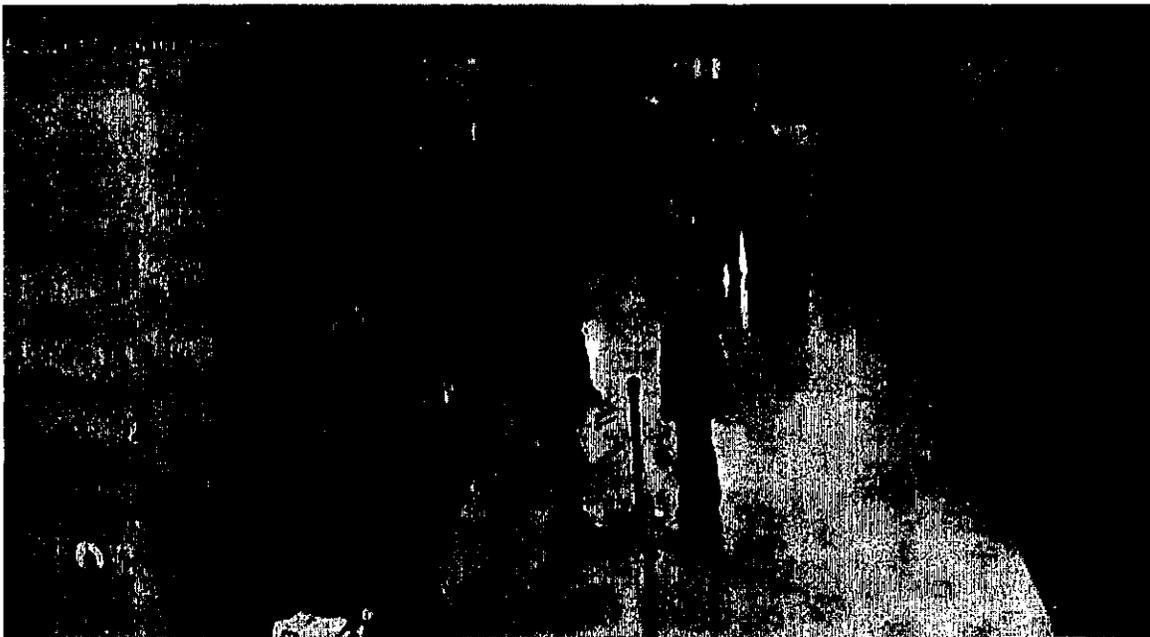
30. The next screenshot is from the elapsed time of 11 minutes and 28 seconds in that video and shows Rachel Atcheson while she worked for the CAU as she illegally refused to let me walk past her to attend the 5/23/17 public resource fair meeting as she instead made hand and arm gestures to me and otherwise told me to move away from a short public corridor that leads to the VMH in which that meeting was then being held.



31. Ms. Atcheson now works for the Mayor's Office as a senior assistant to Eric Adams. On 6/27/22, I legally recorded an audio recording at 4:17 pm inside of a small conference room located in City Hall as I met with New York City Mayor Eric Adams after having just testified to him in the Blue Room in City Hall during a public hearing that was recorded on video as a result of arrangements that were made by the Mayor's Office. That video recording is available at https://www.youtube.com/watch?v=rAye14zJr_Q and my testimony then begins at the elapsed time of 5 minutes and 17 seconds in that video. A copy of the audio recording to which I just referred is available at <https://drive.google.com/file/d/1cC5ABgu1g3tLKgtBngdeI9U0JbE9yqCW/view?usp=sharing>. That audio recording confirms that he made remarks to me at the elapsed times of a) 3 minutes and 11 seconds, b) 3 minutes and 15 seconds, and c) 3 minutes and 43 seconds as he condoned the fact that Ms. Atcheson and members of Mr. de Blasio's NYPD security detail were among City of New York personnel who illegally prevented me from lawfully attending the 5/23/17 public resource fair meeting inside of the BSC. In short, his remarks to me then about that were that personnel of the Mayor's Office are required to obey NYPD directives without regard to

whether such directives are illegal and pretextual. He also told me during that meeting that he would look into information that I provided to him then about the fact that personnel of HRA and Urban subjected me to the B&S and that HRA illegally wasn't complying with my discovery rights in K4. Hindsight strongly suggests that he lied to me about that.

32. The next screenshot is from the elapsed time of 16 minutes in that video and shows me as I stood near a censor in journalism named Michael Gartland while he then worked for the New York Post. I was telling him then that I was illegally being prevented from attending the 5/23/17 public resource fair meeting at a time when I was then suing HRA. The material fact that he, the New York Post, nor any other so-called news organization and so-called reporters ever reported anything about the fact that I was illegally barred from public meetings that were public forums underscores my point about the material and indisputable fact that the so-called press aren't surrogates for the general public in gathering and disseminating information. Also, Judge Schofield fraudulently concealed Mr. Gartland's name in her 9/30/19 decision in K5.

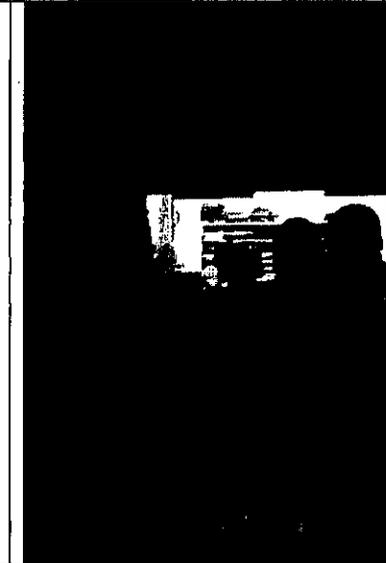


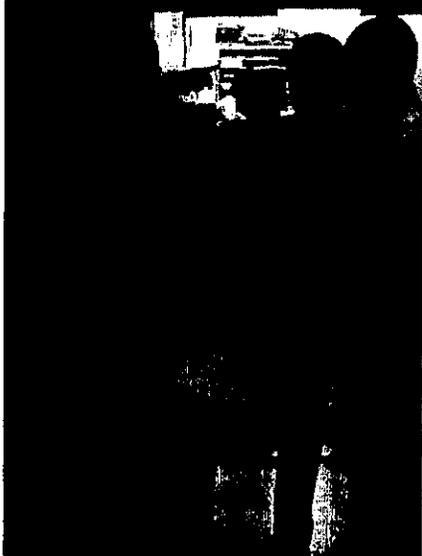
33. On 5/23/17, I also recorded a video with my cell phone at 9:40 am of Mr. Brunner, Mr.

Dominguez and NYPD Officers Ralph Nieves, Raymond Gerola, and Andrew Berkowitz while those members of the NYPD were part of the NYPD security detail for Mr. de Blasio and were acting in concert with Mr. Brunner, Mr. Dominguez, and Mr. Manzi to criminally prevent me from both a) attending the 5/23/17 public resource fair meeting and b) otherwise lawfully standing in the short public corridor that leads to the VMH. I sought to stand there then while not impeding pedestrian traffic partly to engage in expressive association with passerby that partly included members of the public partly about the fact that I was then being illegally discriminated against by such government personnel in a public courthouse and in a public hallway in relation to a public meeting leading up to the 2017 New York City government elections while that public meeting and others were being used as badly disguised campaign events by incumbents and their supporters to attract publicity. Prior to 5/23/17, both Mr. Gerola and Mr. Berkowitz were personally involved with Mr. Redmond in illegally preventing me from lawfully entering the public school that hosted the 4/27/17 town hall meeting in Long Island City in Queens to attend the public town hall meeting that was held there. That confirms that there acts against me on 5/23/17 were a continuing violation.

34. The video that I just discussed and recorded on 5/23/17 at 9:40 am is available at https://drive.google.com/file/d/13_1rNPxqQCYTiskh67jwd-L4hNR9L8hH/view?usp=sharing. While I recorded that video, I did so in an area where I noticed another video security camera that OCA controls and was legally required to have provided video recordings from in response to the FOIL demand that I submitted to it for video recordings that were recorded on 5/23/17 inside of the BSC on its first floor. However, OCA illegally didn't provide me any video recordings from that specific video security camera that may possibly have had its camera angled in a manner that would have recorded those who were recorded by the video that I recorded on

5/23/17 at 9:40 am with my cell phone. This is relevant partly because it supports my point about the material fact that restrictions about taking photographs, recording video recordings, and recording audio recordings inside of public areas inside of state courthouses in New York State outside of courtrooms are illegally largely because those restrictions illegally obstruct people whose rights are violated by New York State court officers and others in such areas to record video recordings, take photographs, and record audio recordings in such areas to gather incontrovertible evidence about that while that may then be provided partly to actual journalists and prosecutors to have such people who commit illegal acts inside of courthouses held properly and promptly accountable. What appears next are a) screenshots from that video, b) information about the elapsed times in that video to which they correspond, and c) information about those who are shown in those screenshots from left to right.

<p>Elapsed time: 4 seconds</p>	<p>Elapsed time:6 seconds</p>
<p>People shown in this screenshot: NYPD Lieutenant Ralph Nieves, NYPD Detective Andrew Berkowitz, New York State court officer Ramond Dominguez, NYPD Detective Raymond Gerola, New York State court officer Matthew Brunner</p>	<p>People shown in this screenshot: Mr. Dominguez , Mr. Nieves, Mr. Berkowitz, Mr. Gerola, Mr. Brunner</p>
	

<p>Elapsed time: 4 seconds</p> <p>People shown in this screenshot: Mr. Nieves, Mr. Berkowitz, Mr. Gerola, Mr. Brunner</p>	<p>Elapsed time:9 seconds</p> <p>People shown in this screenshot: Mr. Nieves, Mr. Gerola, Mr. Brunner, Mr. Berkowitz,</p>
	

35. Steven Banks attended the 5/23/17 public resource fair meeting in the BSC. When I attempted to also lawfully attend that public meeting, I sought to do so partly to talk with him then and while recording and audio or video recording of that to follow-up with him partly about the fact that a) Mr. Mosczyc illegally stole my scheduled 4/12/17 oral arguments hearing in K1 and b) HRA had been proving that its personnel had committed fraud on the court in both K1 and K4. HRA did so by actually and continuously paying for storage unit rental expenses on my behalf to Cubesmart for the storage unit that I continued to rent from it while I resided in my old Urban apartment. HRA paid for such expenses for the entire storage unit rental period between September of 2016 thru to May of 2017. That confirmed that Jeffrey Mosczyc and Marin Gerber of HRA had lied in both K1 and K4 partly on 4/7/17 and 4/11/17 by fraudulently claiming that I wasn't eligible and entitled to have HRA to have done that for the storage unit rental period of May of 2016 thru July of 2016 while I resided in my old Urban apartment. Also, the fact that Mr.

Banks is both an experienced attorney who previously was the head of the Legal Aid Society and Jewish explains why Mr. Banks is partly to blame for Mr. Mosczyk having stolen my 4/12/17 oral arguments hearing in K1. Mr. Banks clearly failed to make certain that Mr. Mosczyk was properly supervised to make certain that he wouldn't commit illegal acts and omissions as an attorney for HRA. Also, the fact that Mr. Banks actively participated in a public town hall meeting on 4/13/17 in Staten Island that was recorded on video clearly cuts against Mr. Mosczyk's claim to Judge Bannon that he wouldn't have been able to participate in the 4/12/17 oral arguments hearing in K1 just 1 day before Mr. Banks violated Passover's rules by actively participating in a town hall meeting.

36. Another reason why I sought to attend that 5/23/17 meeting was to follow-up with personnel of the CCRB and DOE partly to have video recording evidence that was recorded on 4/27/17 at the site of the public town hall meeting in Long Island City in Queens to be promptly preserved and provided to both the CCRB and I. The DOE only provided me some of those video recordings and only video that was recorded after 6:30 pm in response to a FOIL demand. The CCRB unconscionably didn't bother to get the DOE to preserve and provide it such video that was recorded there prior to 6:30 pm on 4/27/17. The video recordings from prior to 6:30 pm on 4/27/17 were still available on 5/23/17. Personnel of both the CCRB and DOE attended the 5/23/17 public resource fair meeting.

37. The 2 e-mail messages shown next that were sent between Denis Reo and I are about the fact that New York State court officers illegally prevented me from visiting areas inside of the SC1 on 3/17/21 while it was open for business and that illegal behavior was a continuing violation by New York State court officers that related back to claims against such court officers that I asserted in K1 and K5. Mr. Reo now works for the SC1 as its Chief Court Clerk.

From: Denis Reo <dreo@nycourts.gov>
To: Towaki Komatsu <towaki_komatsu@yahoo.com>
Sent: Wednesday, March 17, 2021 at 10:31:52 AM EDT
Subject: RE: Denial of access to the courts

I apologize. You should not have been prevented from entering the building. I have spoken with the Captain and it will not happen again. Please note though that there are certain departments in the County Clerk's office that are closed on certain days. That is the County Clerk's decision, not the mine.

From: Towaki Komatsu <towaki_komatsu@yahoo.com>
Sent: Wednesday, March 17, 2021 10:17 AM
To: Denis Reo <dreo@nycourts.gov>
Subject: Denial of access to the courts

Mr. Reo,

I was just illegally prevented from using the facilities at 60 Centre Street to prepare legal briefs that are tied to my lawsuit against HRA that I previously contacted you about? The index number of that case is 100054/2017

What can be done about that?

The court officers directed me to contact the chief clerk.

From,

Towaki Komatsu

38. Although I cited remarks that Judge Engoron made I decisions that he issued in Trump1 in my filings in K2, New York State court officers have criminally prevented me from lawfully attending court hearings that have been held in Trump1 from inside of the specific courtroom in which Judge Engoron has conducted Trump1 as such court officers have informed me that the general public has been barred from that courtroom while members of the so-called press were allowed to attend court hearings in Trump1 from inside of that courtroom.

39. On 10/4/23, I legally recorded an audio recording at 2 pm with my cell phone of a conversation that I had with a New York State court officer whose last name is something similar to Holig, is a white male, and is bald. I recorded that audio recording while we stood in the first

floor lobby of the building located at 25 Beaver Street in Manhattan in which OCA has offices. A copy of that audio recording is available at https://drive.google.com/file/d/1YfHI3_Ko-WfWUg8BxqouoWkuiFt3G1k0/view?usp=sharing. Shortly after I finished talking with him, I left that building and took a photograph at 2:04 pm of the exterior of it to be able to confirm where I had just been. The screenshot shown next is from that photograph.



40. The following is true about what is heard in the audio recording that I recorded at 2 pm on 10/4/23 to which I just referred above:

a. He is heard at the elapsed time of roughly 35 seconds as he stated my last name in spite of the fact that I hadn't previously met him and hadn't otherwise identified myself to anyone when I visited that building on that date. This sufficiently establishes a very strong likelihood that personnel of OCA have subjected me to discriminatory surveillance and profiling without any valid legal grounds. In fact, he also rhetorically asked me then about who didn't know me.

b. He is heard at the elapsed time of 45 seconds as he refused to grant me authorization to take a photograph of his uniform and the court officer shield on it that identified himself. I had just asked him for permission to photograph that.

c. He is heard at the elapsed time of 1 minute and 6 seconds as he interrupted a question that I was asking him by telling me that a decision that the U.S. Secret Service made was responsible for why the general public was being prevented from lawfully attending public court hearings that were being held inside of the specific courtroom in which Judge Engoron was present while conducting them in Trump1. The question that I began to ask him when he interrupted me was about why members of the so-called press were being allowed to be in that specific courtroom while the general public was being illegally and discriminatorily barred from it without any due process in that regard and after such members of the general public would have necessarily needed to complete a standard security screening check upon entering the SC1.

d. I'm heard clearly asking him at the elapsed time of 1 minute and 8 seconds why the so-called press was being permitted to be in that specific courtroom while the general public was being barred from it. In response, he is heard at the elapsed time of 1 minute and 10 seconds as he told me that the press was covering that case and further stated that it had been decided that the press didn't pose a security risk and that was why the press was allowed to be in that courtroom for Trump1.

e. I'm heard at the elapsed time of 1 minute and 17 seconds as I immediately countered his claim by asking him to disclose to me what the security risk about the public was that was causing the general public to be barred from that same courtroom given the material fact that the general public is required to undergo a standard security screening upon entering the SC1. In response, he ducked that question while irrelevantly stating that a decision had been made by the U.S. Secret Service and New York State court officers to allow the press to enter that courtroom for Trump1.

f. I'm heard at the elapsed time of 1 minute and 37 seconds as I asked him to

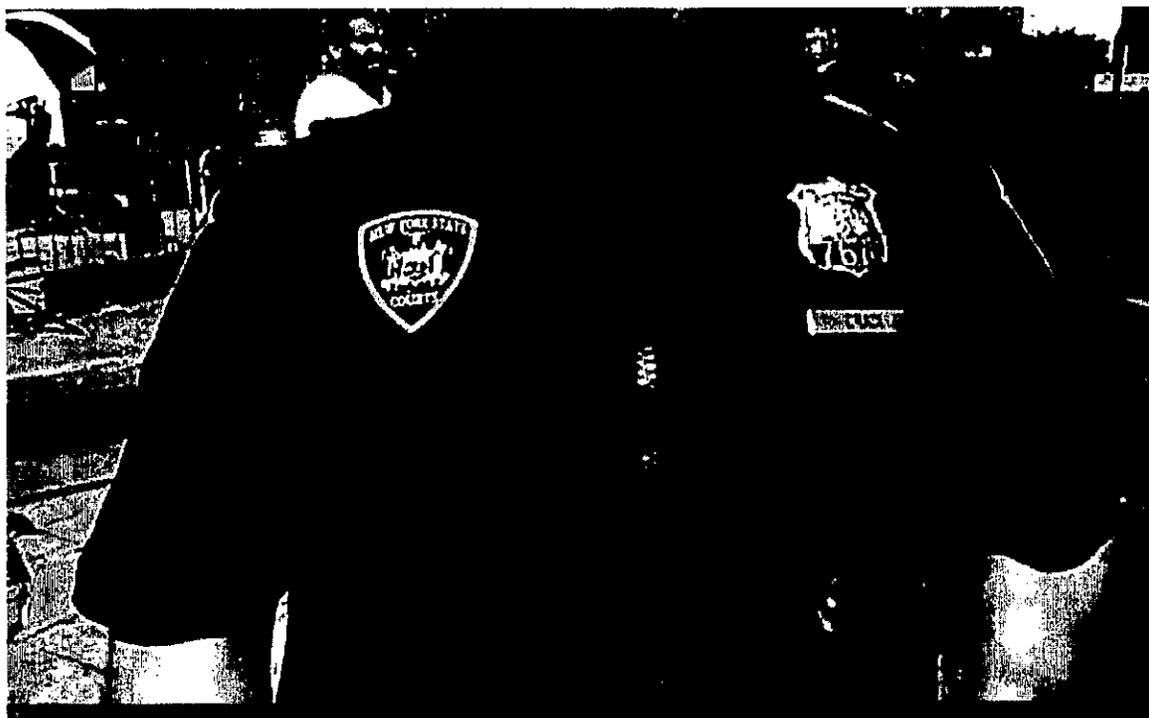
identify the specific people who made that decision to exclude the general public from that courtroom to enable me to identify defendants for a lawsuit that I intended to file about that. In response, he told me that I could sue both the New York State Court System and the U.S. Secret Service about that.

g. I'm heard at the elapsed time of 1 minute and 58 seconds as I told him that New York State court officers had also illegally attempted to coerce me to move away earlier that same day from where I lawfully stood on a public sidewalk located in front of the SC1 in spite of the fact that New York State court officers didn't have any jurisdiction over where I was then standing as I was trying to have face-to-face conversations with journalists who were then nearby. In response, he is heard at the elapsed time of 2 minutes and 14 seconds by fraudulently claiming that New York State court officers had jurisdiction over that area that entitled them to direct me to move away from where I lawfully then stood in what is a traditional public forum.

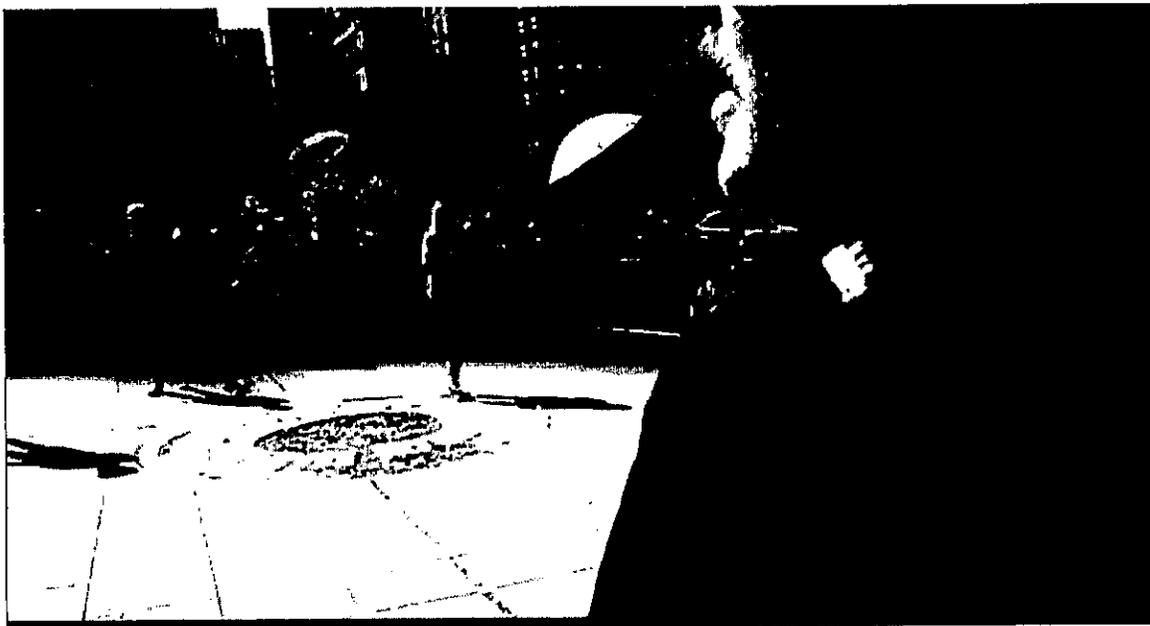
41. At 12:53 pm on 10/4/23, I recorded a video with my cell phone as I stood in an area of a public sidewalk located in front and to the side of the SC1 near where park benches are setup while I wasn't obstructing pedestrian traffic. A copy of that video recording is available at https://drive.google.com/file/d/1d-KlHz_pYg6TDiiksJjWnJ5OnnTnC3-e/view?usp=sharing. The screenshot that is shown next is from the elapsed time of 1 second in that video and confirms that I wasn't in anyone's way nor near the steps to the front of the SC1.



42. The screenshot that is shown next is from the elapsed time of 15 seconds in that video and shows a New York State court officer whose last name is Drain and badge number is 7676 as he illegally tried to coerce me from where I lawfully then stood.



43. The screenshot that is shown next is from the elapsed time of 40 seconds in that video and shows a New York State court officer whose last name is Chester and badge number is 6275 as he also illegally tried to coerce me from where I lawfully then stood. While Mr. Chester and Mr. Drain were illegally harassing me then partly by discriminating against me, metal barricades were setup nearby on that same public sidewalk while members of the so-called press were gathered on the opposite side of them and weren't being told by anyone to leave that sidewalk. The is confirmed by the screenshot shown next that is from the elapsed time of 1 minute and 14 seconds in that video. This fact and circumstance confirms that I had just as much right as those other people to exercise my First and Fourteenth Amendment rights partly of assembly and liberty simply by standing on that public sidewalk without being bothered whatsoever by any court officer nor member of the NYPD.



44. At 12:08 pm on 10/18/23, I recorded a video with my cell phone while standing on a public sidewalk in front of TM while metal barricades were illegally setup in front of me that

prevented me from being able to walk directly to the SC1's front entrance. A copy of that video is available at

<https://drive.google.com/file/d/1nKoVTe8WWSPbfWZx8CL9H5neEVdBufAc/view?usp=sharing>

g and what I just discussed is confirmed by what is shown in that video at the elapsed time of 10 seconds.

45. At 12:10 pm on 10/18/23, I recorded a video with my cell phone while talking with an NYPD officer whose last name is similar to Ciancio and badge number is 13372 near the intersection of Pearl Street and Centre Street in Manhattan. A copy of that video is available at [https://drive.google.com/file/d/1JsWtV_5ADT6-](https://drive.google.com/file/d/1JsWtV_5ADT6-L5FbsOKdn_5AEMemlXqw/view?usp=sharing)

[L5FbsOKdn_5AEMemlXqw/view?usp=sharing](https://drive.google.com/file/d/1JsWtV_5ADT6-L5FbsOKdn_5AEMemlXqw/view?usp=sharing). The following is heard and otherwise shown in that video:

a. I correctly told him at the elapsed time of 39 seconds that the metal barricades that were setup on public sidewalks nearby were violating the Americans with Disabilities Act by. He lied by denying that.

b. I correctly told him at the elapsed time of 46 seconds that I didn't need to tell him where I was then going. To require that would be illegal compelled expression in violation of my privacy and liberty rights as well as my First Amendment rights. He then lied by claiming that I needed to answer his question.

c. He is heard blatantly lying at the elapsed time by fraudulently claiming that unless I had a piece of paper or some notification, I was prohibited from walking past him to visit the SC1.

46. At 12:38 pm on 10/18/23, I recorded a video with my cell phone while talking with a female New York State court officer whose last name is something similar to Figueroa while we

then were in front of the main entrance to the SC1 and I wasn't in anyone's way. A copy of that video is available at <https://drive.google.com/file/d/1Wi-qKJHMvqc7NSQ1SoZYfQdUnbUX9Vsn/view?usp=sharing>. The following screenshot shows her as she illegally discriminated against me by directing me to leave that area in spite of the material fact that people periodically stand in that same general area at various times that partly include while taking wedding and other photographs, filming episodes of "Law and Order", and during rainstorms:



47. When former NYPD Inspector Howard Redmond pled guilty on 8/9/23 inside of the Manhattan Criminal Court to having committed felonies in relation to having obstructed an investigation that was conducted by the New York City Department of Investigations, I attended the court hearing during which he pled guilty. Before that court hearing began, New York State

court officers illegally tried to coerce me to move away from where I lawfully stood and sat in the public hallway located directly outside of the courtroom in which Mr. Redmond pled guilty. That was witnessed by censors in journalism and actual news reporters who were gathered nearby.

48. The following is a relevant excerpt from an e-mail message that a) was sent to me on 10/31/23 at 3:25 pm by someone whose first name is Lhara and works for OTDA that included a copy of the audio recording that OTDA recorded on 10/31/23 of the FH that it briefly conducted by telephone for me against HRA for FH number 8674549L as a resumption of a FH that OTDA conducted on 10/23/23 that shared that same FH number:

From: Hearings, AdminRecords (OTDA) <AdminRecords@otda.ny.gov>
Sent: Tuesday, October 31, 2023 3:25:45 PM
To: 'towaki_komatsu@yahoo.com' <towaki_komatsu@yahoo.com>
Subject: Encrypt:

Good afternoon,

As requested please find the requested Audio for today's hearing attached.

Thank you,

Lhara

49. A copy of the audio recording that OTDA recorded on 10/31/23 for OTDA FH number 8674549L that was attached to the preceding e-mail is available at https://drive.google.com/file/d/1A0FnW_TMUX4yW5gQU-e8hNBguij9h_zP/view?usp=sharing and confirms the following about what is heard in it:

a. The OTDA ALJ who presided over that hearing is heard at the elapsed time of roughly 2 minutes and 11 seconds as he both a) told me that he wouldn't issue a subpoena against HRA on my behalf to order it to provide me the discovery material that I ordered HRA's personnel prior to that FH to provide to me prior to it for that FH and b) told me that he didn't

know whether he had the power to issue such a subpoena in spite of the fact that 18 NYCRR §358-5.6(b)(8)⁴ confirms that OTDA ALJs have that power.

50. The following is a relevant excerpt from an e-mail message that a) was sent to me on 10/27/23 at 9:33 am by Martica Howard of OTDA that included a copy of the audio recording that OTDA recorded on 10/23/23 of the FH that it conducted by telephone for me against HRA for FH number 8674549L and b) I didn't receive for some reason until that e-mail was re-sent to me by her later that day:

From: Hearings, AdminRecords (OTDA) <AdminRecords@otda.ny.gov>
Sent: Friday, October 27, 2023 9:33:07 AM
To: 'towaki komatsu@yahoo.com' <towaki_komatsu@yahoo.com>
Subject: ENCRYPT: FH # 8674549L -AUDIO

Good Morning Mr. Komatsu,
 Please see that I have attached the audio you requested. Have a great day!

Best,
 Martica

51. A copy of the audio recording that OTDA recorded on 10/23/23 for OTDA FH number 8674549L is available at

<https://drive.google.com/file/d/1SOBUskiI4s0CatnE1bwSc0zUybF31X6D6/view?usp=sharing>

and confirms the following about what is heard in it:

b. The OTDA ALJ who presided over that hearing is heard at the elapsed time of roughly 6 minutes and 5 seconds as he both a) told me that he wouldn't issue a subpoena against HRA on my behalf to order it to provide me the discovery material that I ordered HRA's personnel prior to that FH to provide to me prior to it for that FH and b) lied to me by

⁴ This regulation is available on a New York State government web site that is located at <https://regs.health.ny.gov/content/section-358-56-hearing-officer>.

fraudulently claiming that he didn't have the power to issue such a subpoena against HRA. He told me that in response to a question that I had just asked him about whether he would issue a subpoena for that purpose.

c. That OTDA ALJ is heard at the elapsed time of 5 minutes and 12 seconds as he a) informed me that HRA had submitted an evidence packet report to OTDA for that FH that consisted of just 6 pages and b) asked me if I had received it.

d. I'm heard at the elapsed times of a) 4 minutes and 48 seconds and b) 5 minutes and 22 seconds as I told that OTDA ALJ that I hadn't received any discovery material from HRA for that FH. I also clearly told him during that FH that I had submitted a discovery demand to HRA's personnel prior to that FH for that FH that HRA illegally ignored.

e. That OTDA ALJ is heard at the elapsed time of 5 minutes as he informed me that no one who would be representing HRA for that FH would be available for us to talk with during it as he informed me that OTDA had granted HRA a waiver that allowed HRA to instead submit documents for that FH.

f. That OTDA ALJ is heard at the elapsed time of 1 minute and 35 seconds as he told me that I could visit OTDA's office located at 14 Boerum Place in Brooklyn anytime I liked. However, he is then heard at the elapsed time of 2 minutes and 4 seconds as he proved that he had just lied to me by stating then that he just noticed that information that was available to him indicated that I was banned from being able to visit OTDA's offices in Brooklyn at 14 Boerum Place. He told me then that someone from OTDA had coded me as "security violent". This confirms that someone from OTDA subjected me to illegal stigma-plus defamation by making a fraudulent claim about me that contended that I'm a violent person and posed a threat of violence against OTDA and/or HRA personnel.

g. That OTDA ALJ is heard at the elapsed time of 7 minutes and 1 second as he made remarks to me in which he informed me that someone who works for OTDA or previously did so caused me to be banned from being able to participate in fair hearings that OTDA conducts by visiting its offices in Brooklyn that are located at 14 Boerum Place. He elaborated about that somewhat by informing me that whoever made that decision had caused an entry to be recorded in OTDA's records that contended that there was a concern about violence by me after an alleged incident involving me had occurred to allegedly arouse such security concerns. Contrary to that claim, I absolutely never conducted myself in any violent nor threatening manner inside of OTDA's offices nor otherwise made remarks to anyone that suggested that I would engage in violence against anyone who works for OTDA or HRA. Moreover, I participated in a FH remotely for OTDA FH number 8632266M by telephone that OTDA conducted on 7/26/23 against HRA while I sat at a table inside of OTDA's offices in Brooklyn at 14 Boerum Place. This is confirmed by the fact that the OTDA ALJ for that 7/26/23 FH for FH number 8632266M is heard stating "He's at Boerum" about me at the elapsed time of 1 minute and 42 seconds in the audio transcript that OTDA recorded of that 7/26/23 FH that is available at <https://drive.google.com/file/d/1q8bpaK4ZkU8qdkvOgkIBLvxintGLOY8F/view?usp=sharing>.

52. Shortly before I was illegally prevented from attending the public town hall meeting on 4/20/17 that members of the public held partly with Mr. Banks and Mr. De Blasio inside of a public school located in Long Island City in Queens, I was in contact with senior personnel of the New York State Public Advocate's Office partly in April of 2017 in regards to my claims against HRA pertaining to storage unit rental expenses that I paid to Cubesmart for the storage unit rental period of May of 2016 thru July of 2016. In April of 2017, both Jennifer Levy and Muhammad Umair Khan worked for the New York City Public Advocate's Office while Letitia

James was then New York City's Public Advocate. All 3 of them now work for the NYAG. The following e-mail that Ms. Levy sent to me on 4/25/17 at 8:50 am confirms what I just stated about the material fact that I was in contact with her partly about my claims against HRA that concerned storage unit rental expenses just 2 days before I was illegally prevented from attending the 4/27/17 town hall meeting:

From: Jennifer Levy <jlevy@pubadvocate.nyc.gov>
To: "towaki_komatsu@yahoo.com" <towaki_komatsu@yahoo.com>
Cc: Muhammad Umair Khan <khan@pubadvocate.nyc.gov>
Sent: Tuesday, April 25, 2017 at 08:50:47 AM EDT
Subject: Fair hearing at 2:30 today

Good morning Mr. Komatsu,

I reviewed the papers that Mr. Khan sent me. It appears you have two pending Fair Hearings - one that was adjourned on 4/11/2016 and one that is scheduled for today. They both appear to be about storage. What is the prejudice to you in going forward with today's hearing? And, if there is prejudice, can you not either seek an adjournment or withdraw your hearing request without prejudice and start anew? Also, are you considering appealing the 4/19/2017 decision? You will need to do that if you want to address the May - July storage that HRA refused to pay.

--

Jennifer Levy
 General Counsel - Litigation
 Office of NYC Public Advocate Letitia James
 1 Centre Street, 15th Floor North, New York, NY | 10007
 Office: (212) 669-2175
 Email: JLevy@pubadvocate.nyc.gov
<http://www.pubadvocate.nyc.gov/>
 @NYCPA | @JenniferLevy17

53. As shown in the preceding e-mail, Ms. Levy was the General Counsel of the New York City Public Advocate's Office then and she is now the head of the NYAG's Public Integrity division. It's very likely that the actual rationale for why City of New York personnel illegally prevented me from attending the 4/27/17 town hall meeting that I discussed was partly due to

interactions that I had with the New York City Public Advocate’s Office in April of 2017 about and against HRA concerning claims about storage unit rental expenses that I asserted in both K1 and K4 prior to 4/27/17 that the New York City Public Advocate’s Office had been in contact with personnel of HRA about. Concerning this point, the second exhibit that appears within the annexed Exhibit A are copies of 2 e-mails that a man named Fernando Fernandez sent on 4/24/17 at 5:08 pm and 2/8/17 at 3:21 pm partly to Ms. Levy, Ann Marie Scalia of HRA, and personnel of OTDA concerning my claims against HRA about storage unit rental expenses that I paid to Cubesmart for the storage unit rental period of May of 2016 thru July of 2016.

Sworn to before me on the 3rd day of November, 2023

State of New York
County of New York



Notary Public

Towaki Komatsu

DANIEL T. CHENG
NOTARY PUBLIC, STATE OF NEW YORK
REG. NO 04CH0015293
QUALIFIED IN NEW YORK COUNTY
COMMISSION EXPIRES OCTOBER 30, 2027

Exhibit A

**STATE OF NEW YORK
UNIFIED COURT SYSTEM
UNUSUAL OCCURRENCE REPORT**

DATE OF OCCUR.	TIME	COURT/FACILITY	PLACE OF OCCURRENCE	UNUSUAL NUMBER		
				LOC. CODE	REP. NO	YEAR
05/23/2017	0950	BRONX SUPREME COURT - GRAND CONCOURSE	MAGNETOMETER POST D	G	75089	2017
NATURE OF UNUSUAL OCCURRENCE						
<input type="checkbox"/> ARREST <input type="checkbox"/> ATTEMPTED ESCAPE <input type="checkbox"/> BOMB THREAT <input type="checkbox"/> DISRUPTIVE PRISONER <input type="checkbox"/> DISRUPTIVE SPECTATOR <input type="checkbox"/> JUDICIAL THREAT <input type="checkbox"/> PRISONER ESCAPE <input type="checkbox"/> PROPERTY DAMAGE <input type="checkbox"/> PROPERTY THEFT <input type="checkbox"/> REPORT OF CRIME <input type="checkbox"/> SUMMONS <input checked="" type="checkbox"/> OTHER (SPECIFY BELOW) <div style="text-align: center;">DENIED ENTRY</div>						
LASTNAME UNK.		FIRSTNAME		M.I.	EMPLOYEE NO	SEX M
ADDRESS						
LASTNAME		FIRSTNAME		M.I.	EMPLOYEE	SEX AGE
ADDRESS						
DETAILS: (Include pertinent information regarding nature of unusual occurrence. If arrest, include Arrest No., Pct., Charges, Complainant's Name and Address, Court, Judge, Disposition) AT ABOVE T/P/O, THE ABOVE UNKNOWN SUBJECT WAS DENIED ENTRY INTO A CITY HALL EVENT BEING HELD IN THE ROTUNDA BY CITY HALL STAFF AND MAYOR DEBLASIO'S NYPD DETAIL. SUBJECT WAS ASKED TO VACATE THE AREA HE WAS STANDING IN BECAUSE HE WAS BLOCKING PEDESTRIAN TRAFFIC TO BOTH THE EVENT IN THE ROTUNDA AND ACCESS TO THE PUBLIC ELEVATORS. AFTER SOME RESISTANCE TO THIS REQUEST, SUBJECT DID COMPLY BUT MOVED INTO A MAGNETOMETER PROCESSING AREA. SUBJECT WAS ASKED TO MOVE FROM THIS AREA, AND ONCE AGAIN COMPLIED AFTER SOME INITIAL RESISTANCE.						
NAME AND ADDRESS OF WITNESS <div style="text-align: center;">RAMON DOMINGUEZ SGT. SH. #508</div> <div style="text-align: right;">.... Continue to next page</div>						
SUBMITTED BY ANTHONY MANZI		TITLE CAPTAIN		SHIELD NO. 182		DATE 05/24/2017
REPORTED TO OSTACIO NEGRON		TITLE MAJOR		SHIELD NO. 31		DATE 05/24/2017
APPROVED BY FRANK ZALOGA		TITLE		SHIELD NO.		DATE 06/28/2017
LINKED REPORTS 75377						

FINAL APPROVED

A1

Page 1



**STATE OF NEW YORK
UNIFIED COURT SYSTEM
UNUSUAL OCCURRENCE REPORT**

REPORT ID: 75089

ContinuationNAME AND ADDRESS OF WITNESS

*MATHEW BRUNNER
SGT. SH. #478*

FINAL APPROVED

A1

Page 2

From: Fernando Fernandez [mailto:ffernandez@pubadvocate.nyc.gov]
Sent: Monday, April 24, 2017 5:08 PM
To: Best-Childers, Jacqueline (HRA) <best-childersj@hra.nyc.gov>; Scalia, Ann Marie (HRA) <scallaa@hra.nyc.gov>;
Donovan, Jackie (OTDA) <Jackie.Donovan@otda.ny.gov>
Cc: Julissa Gonzalez <jgonzalez@pubadvocate.nyc.gov>; Jennifer Levy <jlevy@pubadvocate.nyc.gov>; Tai Johnson
<tjohnson@pubadvocate.nyc.gov>
Subject: RE: Won HRA Fair Hearing, HRA Has Not Paid Storage Fees

RE: Mr. Towaki Komatsu, HRA - Won Fair Hearing to pay for Storage Fees
HRA ID#: 00037876365A
Center: 46
Fair Hearing #: 00037876365A, Decision dated 09/15/2016
Address: One Penn Plaza, # 6321
New York, NY 10119
Tel. 201-315-5484

Ms. Best-Childers & other HRA / OTDA Staff:

This is the third request that our office has submitted to HRA requesting resolution on the Fair Hearing decision won by our constituent referenced above on 09/15/2016 to pay storage fees. These storage fees keep accumulating as we speak & our constituent is more frustrated as the days go by.

Can you please share with our office the reasons that have caused these numerous delays. We appreciate your prompt response.

Fernando

Fernando Fernandez

Deputy Director of Constituent Services
Office of the Public Advocate Letitia "Tish" James
1 Centre Street N., 15th Floor
New York, NY 10007
Tel. 212-669-3571
Fax 212-669-4701
ffernandez@pubadvocate.nyc.gov

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential, personal, private, sensitive and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including, but not limited to, the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender immediately to notify him/her of the misdirection and destroy all copies of the communication.

NYC Public Advocate Mail - RE: Won Fair Hearing on 09/15/2016, HRA ignores OTDA... Page 1 of 1



**NYC
Public
Advocate**

Fernando Fernandez <ffernandez@pubadvocate.nyc.gov>

RE: Won Fair Hearing on 09/15/2016, HRA ignores OTDA Decision to reimburse \$1,300 for storage fees

1 message

Fernando Fernandez <ffernandez@pubadvocate.nyc.gov>

Wed, Feb 8, 2017 at 3:21 PM

To: [REDACTED]@hra.nyc.gov

Cc: Christopher Donald <cdonald@pubadvocate.nyc.gov>, George Haigler <ghaigler@pubadvocate.nyc.gov>

RE: Mr. Towaki Komatsu, HRA ID#: 00037876365A
Center #: 46
Fair Hearing #: 7316477K, Decision dated 09/15/2016
One Penn Plaza, Suite 6321
New York, NY 10119
Tel. 201-315-5484

Attention: [REDACTED]

Our office is reaching out to you as our constituent had won an OTDA, Fair Hearing Decision on 09/15/2016 to process & reimburse \$1,300 out of pocket expenses (that he still owes) to retrieve personal belongings in storage due for auction. HRA has ignored our constituent's numerous attempts with the local HRA Center to be process for the reimbursement. In turn, he is met with disdain & non-compliance. It has been almost 5 months after the OTDA Decision, yet no one step has been taken by the local HRA Center.

We have attached a copy of the OTDA Decision for your review.

As always, thank you for all your assistance.

Fernando Fernandez
Deputy Director of Constituent Services
Office of the Public Advocate Letitia "Tish" James
1 Centre Street N., 15th Floor
New York, NY 10007
Tel. 212-669-3571
Fax 212-669-4701
(PA Case #: 125393)
ffernandez@pubadvocate.nyc.gov
Attachment

Towaki Komatsu HRA - Won Fair Hearing, see OTDA Decision.pdf
1023K

A2

<https://mail.google.com/mail/u/0/?ui=2&ik=a9d8ea7bad&view=pt&search=sent&th=15a1f6...> 2/8/2017

**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: Commissioner Jocelyn Strauber

Address: Department of Investigation

I represent: 180 Maiden Lane

Address: NY, NY 10038

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 1207/1193 Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Ivy Dyson

Address: _____

I represent: Brennan Center for Justice

Address: 120 Broadway

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 1207/1193 Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: NINA LUSHKAJIAN

Address: _____

I represent: SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

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: Elizabeth Vasquez - BDS

Address: _____

I represent: Brooklyn Defender Services

Address: BK

**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: 12/15/93

(PLEASE PRINT)

Name: Michael Smitzky

Address: _____

I represent: New York Civil Liberties Union

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: Elizabeth Daniel Vasquez

Address: _____

I represent: Brooklyn Defenders

Address: 127 Livingston, Brooklyn

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: 12/15/23

(PLEASE PRINT)

Name: Agency Chief Contracting Officer Nicoles Mendoza

Address: NYPD

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: 12/15/23

(PLEASE PRINT)

Name: Michael Fitzpatrick

Address: 15 arched Center, Brooklyn

I represent: Office of Technology & Innovation

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: 12/15/23

(PLEASE PRINT)

Name: Managing Attorney Melanie Bravenman

Address: NYPD

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. _____ Res. No. _____

in favor in opposition

Date: 12/15/23

(PLEASE PRINT)

Name: Chief Privacy Officer Emily Gold

Address: NYPD

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: Asst. Deputy Commissioner Seth Severino

Address: NYPD

I represent: _____

Address: _____

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 1193, 1195, 1207 Res. No. _____

in favor in opposition

Date: 12/15/23

(PLEASE PRINT)

Name: Chief Jeffrey Maddrey

Address: NYPD

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. 1195, 1195, 1207 Res. No. _____

in favor in opposition

Date: 12/15/23

(PLEASE PRINT)

Name: Deputy Commissioner Michael Gerber

Address: NYPD

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: 12/15/2023

(PLEASE PRINT)

Name: Jerame 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. _____ Res. No. _____

in favor in opposition

Date: 12/15/23

(PLEASE PRINT)

Name: Jonathan Lam

Address: _____

I represent: Amnesty International USA

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: _____

Name: Andrew

(PLEASE PRINT)

Address: _____

I represent: SELF

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: 12/13/23

Name: Josiah Komertser

(PLEASE PRINT)

Address: _____

I represent: SELF

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: 12/15/23

Name: Raul Rivera

(PLEASE PRINT)

Address: _____

I represent: _____

Address: _____

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